PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-255431
(43)Date of publication of application : 19.09.2000

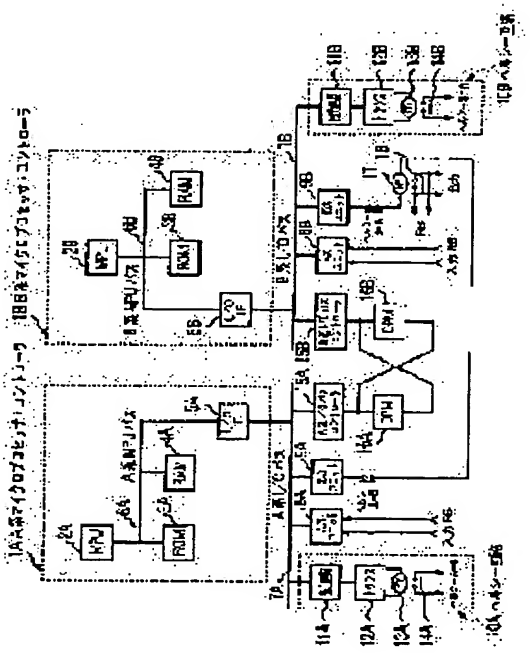
(51)Int.CI. B61L 23/04
G05B 9/03

(21)Application number : 11-055774
(22)Date of filing : 03.03.1999

(71)Applicant : EAST JAPAN RAILWAY CO
TOSHIBA CORP
(72)Inventor : ICHIKAWA NORIAKI
MEGURO TAKAYUKI
OTANI YOSHIYUKI
ISONO KYOSUKE
NAGASHIMA TERUZO
YASUMOTO TAKANORI

(54) SAFETY CONTROL DEVICE FOR AND SAFETY CONTROL SYSTEM OF RAILWAY

(57)Abstract:
PROBLEM TO BE SOLVED: To enhance fail safe with a simple configuration.
SOLUTION: Input units 8A, 8B apply input signals from on-site devices to controllers 1A, 1B, respectively. The controllers 1A, 1B carry out operation based on the inputs of the signals to apply control signals to the on-site devices via output units 9A, 9B. In carrying out an input process, an operation process, and an input process, the controllers 1A, 1B carry out the collation of a self system and a mating system through common memories 16A, 16B. Disagreed data finds a fault to stop running. Healthy circuits 10A, 10B are circuits for applying signals indicating that the self system is in health. Applying signals indicating that any one of the systems is in abnormal applies no signals from the output units 9A, 9B.



LEGAL STATUS
[Date of request for examination] 05.09.2002
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）

(12) 公開特許公報（Ａ）

(11)特許出願公開番号
特開2000－255431
（P2000－255431A）

(43)公開日　平成12年９月19日(2000.9.19)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｂ６１Ｌ　23/04		Ｂ６１Ｌ　23/04	５Ｈ２０９
Ｇ０５Ｂ　9/03		Ｇ０５Ｂ　9/03	

審査請求　未請求　請求項の数15　ＯＬ　（全 22 頁）

(21)出願番号　特願平11－55774

(22)出願日　平成11年３月３日(1999.3.3)

(71)出願人　000221616
東日本旅客鉄道株式会社
東京都渋谷区代々木二丁目二番二号

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　市　川　憲　照
東京都渋谷区代々木二丁目２番２号　東日本旅客鉄道株式会社内

(74)代理人　100064285
弁理士　佐藤　一雄　（外３名）

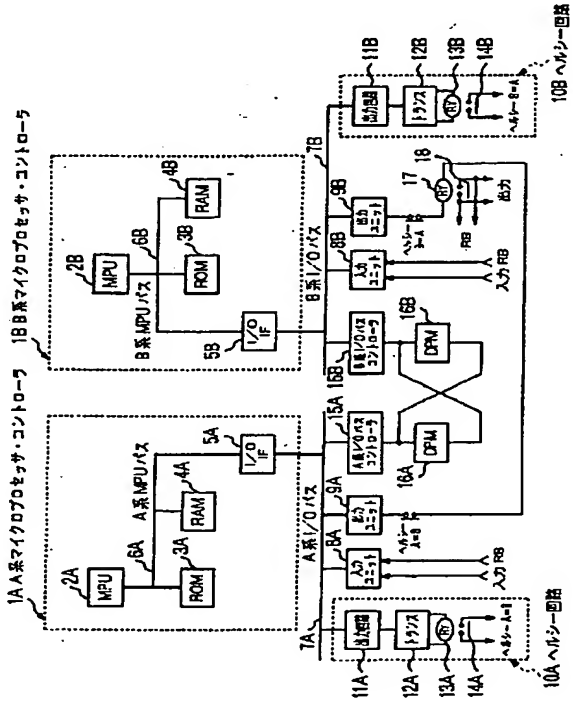
最終頁に続く

(54)【発明の名称】　鉄道用保安制御装置及び保安制御システム

(57)【要約】

【課題】　簡単な構成によって、フェイルセーフ性を向上させること。

【解決手段】　入力ユニット８Ａ，８Ｂは、それぞれ現場機器からの入力信号をコントローラ１Ａ，１Ｂに出力する。コントローラ１Ａ，１Ｂはこの信号の入力に基づき演算を行い制御信号を出力ユニット９Ａ，９Ｂを介して現場機器に出力する。コントローラ１Ａ，１Ｂは、入力処理、演算処理、及び出力処理を行うに際して、共有メモリ１６Ａ，１６Ｂを通して互いに自系と他系との照合を行い、データが一致しない場合は故障であるとして走行を停止する。ヘルシー回路１０Ａ，１０Ｂは自系が健全であることを示す信号を出力する回路であり、一方が異常を示す信号を出力すると出力ユニット９Ａ，９Ｂから信号が出力されない。



【特許請求の範囲】
【請求項１】現場機器に対する制御が可能な少なくとも２系統以上の制御系を有し、この２系統以上の制御系はそれぞれに専用のマイクロプロセッサ・コントローラを有している鉄道用保安制御装置において、
前記各制御系は、
自系統側及び１つの他系統側の入出力結果を記憶し、前記現場機器との間の信号の入出力結果について、自系統側と１つの他系統側との間で一致するか否かを照合するための共有メモリと、自系統側又は照合相手の他系統側が正常状態又は故障状態のいずれにあるかを示す信号を出力するヘルシー回路と、を有しており、
各制御系の前記マイクロプロセッサ・コントローラは、前記共有メモリを用いて前記照合を行い、その照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行すると共に、自系統側又は１つの他系統側のいずれかのヘルシー回路から故障状態を示す信号を入力した場合は、その制御動作を停止するものであり、
前記ヘルシー回路は、交番信号を出力する交番信号出力回路と、前記交番信号出力回路からの交番信号を１次側に入力し２次側から交番信号の交流分のみを出力するトランスと、前記トランスからの交番信号を整流した入力により動作するヘルシーリレー接点と、を有するものである、
ことを特徴とする鉄道用保安制御装置。
【請求項２】前記各制御系は、前記現場機器からの信号を入力する専用の入力ユニットを有するものであり、
さらに、各制御系のマイクロプロセッサ・コントローラは、それぞれ自系統側の故障を診断する機能を備えると共に、１つの他系統側の故障診断結果との照合を行う機能を備えており、
自系統側の入力ユニットの入力信号と１つの他系統側の入力ユニットの入力信号とが一致しない場合は、双方の制御系の制御動作を停止し、前記両機能に基づいて危険側故障を確実に検出するようにした、
ことを特徴とする請求項１記載の鉄道用保安制御装置。
【請求項３】前記各制御系の入力ユニットは、前記現場機器からの信号入力経路上に設けられた入力用半導体素子と、この入力用半導体素子に直列接続されたチェック用半導体素子とを有しており、
前記各制御系のマイクロプロセッサ・コントローラは、前記入力用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を行うチェック信号発生回路を有するものである、
ことを特徴とする請求項２記載の鉄道用保安制御装置。
【請求項４】前記各制御系は、前記現場機器に対する出力信号を出力し、且つその信号出力経路が互いに直列接続されている専用の出力ユニットを有するものであり、
自系統側の出力ユニットの出力信号と１つの他系統側の出力ユニットの出力信号とが一致しない場合は、双方の制御系の制御動作を停止するようにした、
ことを特徴とする請求項１乃至３のいずれかに記載の鉄道用保安制御装置。
【請求項５】前記各出力ユニットは、それぞれ前記信号出力経路上に設けられた出力用半導体素子と、この出力用半導体素子のオンオフ状態とは反対のオンオフ状態を示す故障検出用半導体素子と、この故障検出用半導体素子に流れる電流を定期的にオンオフさせてこの故障検出用半導体素子自体の故障の有無をチェックするチェック用半導体素子と、を有しており、
前記各マイクロプロセッサ・コントローラは、前記出力用半導体素子をオンオフさせる出力信号駆動回路と、前記故障検出用半導体素子のオンオフ状態の検出により前記出力用半導体素子についての故障の有無を検出する故障検出回路と、前記故障検出用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を定期的に行うチェック信号発生回路と、前記現場機器のリレー接点状態を読み取る接点リードバック回路と、を有しており、これら各回路の入力状態又は出力状態に基づいて、前記各出力ユニットについての故障状態を判別するものである、
ことを特徴とする請求項４記載の鉄道用保安制御装置。
【請求項６】前記各マイクロプロセッサ・コントローラは、前記自系統側の出力ユニットの出力用半導体素子又は前記１つの他系統側の出力ユニットの出力用半導体素子のいずれか一方が半導通状態にあることを検出可能なものである、
ことを特徴とする請求項５記載の鉄道用保安制御装置。
【請求項７】前記各制御系のマイクロプロセッサ・コントローラは、メインプログラムを実行する制御処理手段と、前記メインプログラムに所定時間毎に割り込みプログラムの割り込みをかけて前記交番信号を発生させる交番信号発生手段とを有し、
前記制御処理手段及び前記交番信号発生手段は、前記メインプログラムの１回の処理時間における割込プログラムの割込回数をそれぞれ監視し、この割込回数の値が所定範囲外となった場合に、マイクロプロセッサ・コントローラの制御を停止させるものである、
ことを特徴とする請求項１記載の鉄道用保安制御装置。
【請求項８】前記共有メモリは、前記自系統側又は前記１つの他系統側のマイクロプロセッサ・コントローラのうちのいずれかのプログラム内容の一部が書き換えられた場合に、その書き換えられた内容を記憶可能なものであり、
前記自系統側又は前記１つの他系統側のマイクロプロセッサ・コントローラのうちのいずれか一方のプログラム内容の一部が書き換えられた場合には、他方のプログラム内容も同様に書き換えられるようになっている、
ことを特徴とする請求項１乃至７のいずれかに記載の鉄道用保安制御装置。

【請求項９】前記制御系のいずれかに故障が発生した場合、その制御系のマイクロプロセッサ・コントローラを他の制御系から強制的に切断するため、このコントローラの電源回路をオフにすることによりこのコントローラの動作を停止させる、
ことを特徴とする請求項１乃至８のいずれかに記載の鉄道用保安制御装置。
【請求項１０】前記制御系が第１乃至第３の３つの制御系により構成され、いずれか１つの制御系に故障が発生した場合に、残りの２つの制御系に故障が発生していないことを前記照合機能を用いて検出したときのみ、この残りの２つの制御系により前記現場機器に対する制御を継続する、
ことを特徴とする請求項１記載の鉄道用保安制御装置。
【請求項１１】前記第１乃至第３の３つの制御系の全てによる制御動作実行中に、いずれか２つの制御系が残りの制御系の故障を検出した場合は、残りの１つの制御系のマイクロプロセッサ・コントローラの電源回路がオフとなり、
また、前記第１乃至第３の３つの制御系のうちのいずれか２つの制御系による制御動作実行中に、一方の制御系が他方の制御系の故障を検出した場合は、双方の制御系のマイクロプロセッサ・コントローラの電源回路がオフとなる、
ことを特徴とする請求項１０記載の鉄道用保安制御装置。
【請求項１２】前記各制御系のマイクロプロセッサ・コントローラは、タイマのカウント値に基づきメインプログラムにおける所定動作実行時点を決定し、この時点で前記自系統側と１つの他系統側との間の照合を行う場合に、この時点から所定時間が経過するまでの期間における照合結果を無効とすることにより、前記自系統側のタイマと１つの他系統側のタイマとの間のカウントタイミングのずれに起因する照合エラーを排除するようにした、
ことを特徴とする請求項１乃至１１のいずれかに記載の鉄道用保安制御装置。
【請求項１３】現場機器との間で信号の授受を行う複数の入出力端末装置と少なくとも１台の制御処理端末装置との間を通信ネットワークで接続し、この制御処理端末装置がこれら複数の入出力端末装置を介して複数の現場機器に対する制御を行う制御システムにおいて、
前記入出力端末装置及び前記制御処理端末装置を、前記請求項１乃至１２のいずれかに記載の鉄道用保安制御装置により構成した、
ことを特徴とする鉄道用保安制御システム。
【請求項１４】前記制御処理端末装置は、現在の列車運行用の第１の制御処理端末装置と、新しい応用プログラムが実装された第２の制御処理端末装置とで構成され、列車運行数が多い時間帯では、第１の制御処理端末装置が全ての入出力端末装置との間で信号の授受を行い、
列車運行数が少ない時間帯では、第１の制御処理端末装置は特定の入出力端末装置との間でのみ信号の授受を行うと共に、第２の制御処理端末装置は残りの入出力端末装置との間で信号の授受を行う、
ことを特徴とする請求項１３記載の鉄道用保安制御システム。
【請求項１５】前記各入出力端末装置は、前記第１の制御処理端末装置又は前記第２の制御処理端末装置のうちのいずれと信号の授受を行うかを決める切換スイッチを有しており、この切換スイッチの制御は前記第２の制御処理端末装置により行われるようになっている、
ことを特徴とする請求項１４記載の鉄道用保安制御システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、鉄道用保安制御装置及び保安制御システムに関するものである。
【０００２】
【従来の技術】一般に、鉄道用列車の制御装置に対しては、万一故障が発生したとしても、その装置は常に安全側の状態となるようにして、危険側の状態になるのを回避できるような機能が要求されており、このような機能をフェイルセーフ機能と呼んでいる。例えば、信号制御装置においては、安全側の故障状態とは、列車の進行を許可する信号（青信号）を出力すべきであるにもかかわらず、列車の進行を禁止する信号（赤信号）が誤って出力されているような状態であり、一方、危険側の故障状態とは、列車の進行を禁止する信号（赤信号）を出力すべきであるにもかかわらず、列車の進行を許可する信号（青信号）が誤って出力されているような状態である。また、踏切制御装置においては、安全側の故障状態とは、遮断機を上げる信号を出力すべきであるにもかかわらず、遮断機を下ろす信号が誤って出力されているような状態であり、一方、危険側の故障状態とは、遮断機を下げる信号を出力すべきであるにもかかわらず、遮断機を上げる信号が誤って出力されているような状態である。
【０００３】図１９は、このようなフェイルセーフ機能が要求されている従来の鉄道用保安制御装置の要部の構成を示すブロック図である。この制御装置は、Ａ系及びＢ系から成る２重系の構成を有しており、Ａ系及びＢ系はそれぞれマイクロプロセッサ・ユニット１０１Ａ，１０１Ｂ及びメモリ１０２Ａ，１０２Ｂを有している。これらマイクロプロセッサ・ユニット１０１Ａ，１０１Ｂはクロック回路１０３からのクロック信号により同期を取りながら走行している。
【０００４】マイクロプロセッサ・ユニット１０１Ａ，１０１Ｂにはバス１０４Ａ，１０４Ｂを介してバス照合・交番信号出力回路１０５が接続されている。このバス

照合・交番信号出力回路１０５は、バス１０４Ａ，１０４Ｂ上に現れるマイクロプロセッサ・ユニット１０１Ａ，１０４Ｂの信号を照合し、両者が一致するか否かについてその照合結果を照合異常検出回路１０６に出力している。バス照合・交番信号出力回路１０５は、常時、交番信号を出力しており、両者が一致している場合は、この交番信号の出力を継続することによりマイクロプロセッサ・ユニット１０１Ａ，１０１Ｂの走行を許容する。

【０００５】しかし、バス照合・交番信号出力回路１０５は、両者の信号の不一致が一度でも発生すると、この不一致の情報を記憶し、以後の交番信号の出力を停止する。バス照合・交番信号出力回路１０５からの交番信号の停止で、照合異常検出回路１０６は照合異常を検出し、マイクロプロセッサ・ユニット１０１Ａ，１０１Ｂにリセット信号を出力する。マイクロプロセッサ・ユニット１０１Ａ，１０１Ｂがリセットされることにより、バス照合・交番信号出力回路１０５が照合すべきデータがなくなり、照合不一致となって交番信号を出力できなくなる。

【０００６】そして、双方のマイクロプロセッサ・ユニット１０１Ａ，１０１Ｂはリセットされた状態（安全側の状態となっている）で走行を停止するので、上記のフェイルセーフ機能が確保されることになる。

【０００７】

【発明が解決しようとする課題】従来の鉄道用保安制御装置は、上記したように、図１９のような構成のフェイルセーフ回路によってフェイルセーフ機能が確保されている。しかし、図１９に示したフェイルセーフ回路は、通常、専用のハードウエアにより構成されている。したがって、高性能のマイクロプロセッサ・ユニットやマイクロコンピュータが開発される度に、その都度専用のハードウエアを開発しなければならず、多大の労力及びコストを費やす結果となっていた。

【０００８】また、最近の鉄道用保安制御装置には多くの個所に半導体素子が使用されているが、これらの半導体素子の故障の発生場所あるいは発生態様によってはフェイルセーフ機能を確保できない場合も考えられ、フェイルセーフ性を一定以上向上させることが非常に困難であった。

【０００９】本発明は、上記事情に鑑みてなされたものであり、簡単な構成によって、フェイルセーフ性を向上させることが可能な鉄道用保安制御装置及び保安制御システムを提供することを目的としている。

【００１０】

【課題を解決するための手段】上記課題を解決するための手段として、請求項１記載の発明は、現場機器に対する制御が可能な少なくとも２系統以上の制御系を有し、この２系統以上の制御系はそれぞれに専用のマイクロプロセッサ・コントローラを有している鉄道用保安制御装置において、前記各制御系は、自系統側及び１つの他系統側の入出力結果を記憶し、前記現場機器との間の信号の入出力結果について、自系統側と１つの他系統側との間で一致するか否かを照合するための共有メモリと、自系統側又は照合相手の他系統側が正常状態又は故障状態のいずれにあるかを示す信号を出力するヘルシー回路と、を有しており、各制御系の前記マイクロプロセッサ・コントローラは、前記共有メモリを用いて前記照合を行い、その照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行すると共に、自系統側又は１つの他系統側のいずれかのヘルシー回路から故障状態を示す信号を入力した場合は、その制御動作を停止するものであり、前記ヘルシー回路は、交番信号を出力する交番信号出力回路と、前記交番信号出力回路からの交番信号を１次側に入力し２次側から交番信号の交流分のみを出力するトランスと、前記トランスからの交番信号を整流した入力により動作するヘルシーリレー接点と、を有するものである、ことを特徴とする。

【００１１】請求項２記載の発明は、請求項１記載の発明において、前記各制御系は、前記現場機器からの信号を入力する専用の入力ユニットを有するものであり、さらに、各制御系のマイクロプロセッサ・コントローラは、それぞれ自系統側の故障を診断する機能を備えると共に、１つの他系統側の故障診断結果との照合を行う機能を備えており、自系統側の入力ユニットの入力信号と１つの他系統側の入力ユニットの入力信号とが一致しない場合は、双方の制御系の制御動作を停止し、前記両機能に基づいて危険側故障を確実に検出するようにした、ことを特徴とする。

【００１２】請求項３記載の発明は、請求項２記載の発明において、前記各制御系の入力ユニットは、前記現場機器からの信号入力経路上に設けられた入力用半導体素子と、この入力用半導体素子に直列接続されたチェック用半導体素子とを有しており、前記各制御系のマイクロプロセッサ・コントローラは、前記入力用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を行うチェック信号発生回路を有するものである、ことを特徴とする。

【００１３】請求項４記載の発明は、請求項１乃至３のいずれかに記載の発明において、前記各制御系は、前記現場機器に対する出力信号を出力し、且つその信号出力経路が互いに直列接続されている専用の出力ユニットを有するものであり、自系統側の出力ユニットの出力信号と１つの他系統側の出力ユニットの出力信号とが一致しない場合は、双方の制御系の制御動作を停止するようにした、ことを特徴とする。

【００１４】請求項５記載の発明は、請求項４記載の発明において、前記各出力ユニットは、それぞれ前記信号出力経路上に設けられた出力用半導体素子と、この出力用半導体素子のオンオフ状態とは反対のオンオフ状態を

示す故障検出用半導体素子と、この故障検出用半導体素子に流れる電流を定期的にオンオフさせてこの故障検出用半導体素子自体の故障の有無をチェックするチェック用半導体素子と、を有しており、前記各マイクロプロセッサ・コントローラは、前記出力用半導体素子をオンオフさせる出力信号駆動回路と、前記故障検出用半導体素子のオンオフ状態の検出により前記出力用半導体素子についての故障の有無を検出する故障検出回路と、前記故障検出用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を定期的に行うチェック信号発生回路と、前記現場機器のリレー接点状態を読み取る接点リードバック回路と、を有しており、これら各回路の入力状態又は出力状態に基づいて、前記各出力ユニットについての故障状態を判別するものである、ことを特徴とする。

【００１５】請求項６記載の発明は、請求項５記載の発明において、前記各マイクロプロセッサ・コントローラは、前記自系統側の出力ユニットの出力用半導体素子又は前記１つの他系統側の出力ユニットの出力用半導体素子のいずれか一方が半導通状態にあることを検出可能なものである、ことを特徴とする。

【００１６】請求項７記載の発明は、請求項１記載の発明において、前記各制御系のマイクロプロセッサ・コントローラは、メインプログラムを実行する制御処理手段と、前記メインプログラムに所定時間毎に割り込みプログラムの割り込みをかけて前記交番信号を発生させる交番信号発生手段とを有し、前記制御処理手段及び前記交番信号発生手段は、前記メインプログラムの１回の処理時間における割込プログラムの割込回数をそれぞれ監視し、この割込回数の値が所定範囲外となった場合に、マイクロプロセッサ・コントローラの制御を停止させるものである、ことを特徴とする。

【００１７】請求項８記載の発明は、請求項１乃至７のいずれかに記載の発明において、前記共有メモリは、前記自系統側又は前記１つの他系統側のマイクロプロセッサ・コントローラのうちのいずれかのプログラム内容の一部が書き換えられた場合に、その書き換えられた内容を記憶可能なものであり、前記自系統側又は前記１つの他系統側のマイクロプロセッサ・コントローラのうちのいずれか一方のプログラム内容の一部が書き換えられた場合には、他方のプログラム内容も同様に書き換えられるようになっている、ことを特徴とする。

【００１８】請求項９記載の発明は、請求項１乃至８のいずれかに記載の発明において、前記制御系のいずれかに故障が発生した場合、その制御系のマイクロプロセッサ・コントローラを他の制御系から強制的に切断するため、このコントローラの電源回路をオフにすることによりこのコントローラの動作を停止させる、ことを特徴とする。

【００１９】請求項１０記載の発明は、請求項１記載の発明において、前記制御系が第１乃至第３の３つの制御系により構成され、いずれか１つの制御系に故障が発生した場合に、残りの２つの制御系に故障が発生していないことを前記照合機能を用いて検出したときのみ、この残りの２つの制御系により前記現場機器に対する制御を継続する、ことを特徴とする。

【００２０】請求項１１記載の発明は、請求項１０記載の発明において、前記第１乃至第３の３つの制御系の全てによる制御動作実行中に、いずれか２つの制御系が残りの制御系の故障を検出した場合は、残りの１つの制御系のマイクロプロセッサ・コントローラの電源回路がオフとなり、また、前記第１乃至第３の３つの制御系のうちのいずれか２つの制御系による制御動作実行中に、一方の制御系が他方の制御系の故障を検出した場合は、双方の制御系のマイクロプロセッサ・コントローラの電源回路がオフとなる、ことを特徴とする。

【００２１】請求項１２記載の発明は、請求項１乃至１１のいずれかに記載の発明において、前記各制御系のマイクロプロセッサ・コントローラは、タイマのカウント値に基づきメインプログラムにおける所定動作実行時点を決定し、この時点で前記自系統側と１つの他系統側との間の照合を行う場合に、この時点から所定時間が経過するまでの期間における照合結果を無効とすることにより、前記自系統側のタイマと１つの他系統側のタイマとの間のカウントタイミングのずれに起因する照合エラーを排除するようにした、ことを特徴とする。

【００２２】請求項１３記載の発明は、現場機器との間で信号の授受を行う複数の入出力端末装置と少なくとも１台の制御処理端末装置との間を通信ネットワークで接続し、この制御処理端末装置がこれら複数の入出力端末装置を介して複数の現場機器に対する制御を行う制御システムにおいて、前記入出力端末装置及び前記制御処理端末装置を、前記請求項１乃至１２のいずれかに記載の鉄道用保安制御装置により構成した、ことを特徴とする。

【００２３】請求項１４記載の発明は、請求項１３記載の発明において、前記制御処理端末装置は、現在の列車運行用の第１の制御処理端末装置と、新しい応用プログラムが実装された第２の制御処理端末装置とで構成され、列車運行数が多い時間帯では、第１の制御処理端末装置が全ての入出力端末装置との間で信号の授受を行い、列車運行数が少ない時間帯では、第１の制御処理端末装置は特定の入出力端末装置との間でのみ信号の授受を行うと共に、第２の制御処理端末装置は残りの入出力端末装置との間で信号の授受を行う、ことを特徴とする。

【００２４】請求項１５記載の発明は、請求項１４記載の発明において、前記各入出力端末装置は、前記第１の制御処理端末装置又は前記第２の制御処理端末装置のうちのいずれと信号の授受を行うかを決める切換スイッチ

を有しており、この切換スイッチの制御は前記第２の制御処理端末装置により行われるようになっている、ことを特徴とする。

【００２５】

【発明の実施の形態】以下、本発明の実施形態を図に基づき説明する。但し、以下の実施形態では、鉄道用保安制御装置及び鉄道用保安制御システムとして、電子踏切制御装置及び電子踏切制御システムを例にとり説明するが、本発明の技術の適用はこれらのみに限定されるわけではなく、信号制御装置及び信号制御システムなどの他の制御装置及び制御システムに適用可能なものである。

【００２６】図１は第１の実施形態の構成を示すブロック図である。この第１の実施形態は、Ａ系（第１の制御系）及びＢ系（第２の制御系）の２つの制御系を有するものである。

【００２７】図１において、まず、Ａ系の構成を説明すると、Ａ系マイクロプロセッサ・コントローラ１Ａはマイクロプロセッサ・ユニット２Ａ、ＲＯＭにより構成された記憶部３Ａ、ＲＡＭにより構成された記憶部４Ａ、入出力インタフェイス５Ａを有しており、これらはＭＰＵバス６Ａにより相互に接続されている。

【００２８】入出力インタフェイス５ＡはＩ／Ｏバス７Ａに接続されており、このＩ／Ｏバス７Ａには、また、入力ユニット８Ａ、出力ユニット９Ａ、及びヘルシー回路１０Ａも接続されている。このヘルシー回路１０Ａは、出力回路１１Ａ、トランス１２Ａ、リレー１３Ａ、及びヘルシーリレー接点１４Ａ等により構成されている。Ｉ／Ｏバス７ＡはＩ／Ｏバスコントローラ１５Ａにより制御されるようになっており、このＩ／Ｏバスコントローラ１５Ａに共有メモリ１６Ａが接続されている。

【００２９】Ｂ系の構成もＡ系と同様であるため、Ｂ系についてはその重複した説明を省略する。出力ユニット９Ａ，９Ｂ間には現場機器のリレー１７が接続されており、そのリレー接点１８のオンオフにより、例えば遮断機の制御が行われるようになっている。そして、リレー接点１８の状態は、リードバック（ＲＢ）信号として入力ユニット８Ａ，８Ｂに入力されるようになっている。

【００３０】マイクロプロセッサ・ユニット２Ａは、データの入出力制御、各種演算、シリアルデータ伝送等を行うものである。記憶部３Ａは、マイクロプロセッサ・ユニット２Ａのプログラムを格納するものであり、この実施形態では電気的な書込・消去が可能なＥＥＰＲＯＭにより形成されている。記憶部４Ａは、ユーザアプリケーション・プログラムとマイクロプロセッサ・ユニット２Ａの動作に必要なメモリである。入出力インタフェイス５Ａは、ＭＰＵバス６ＡとＩ／Ｏバス７Ａとの間のインタフェイスを行うものであり、ゲートアレイにより構成されている。

【００３１】入力ユニット８Ａは、例えば所定区間における列車の存在を知らせる信号、あるいは上述したリードバック信号等を入力し、これをＡ系マイクロプロセッサ・コントローラ１Ａに送出するものである。

【００３２】出力ユニット９Ａは、Ａ系マイクロプロセッサ・コントローラ１Ａからの制御信号を出力し、リレー１７の制御を行うものである。但し、後述するように、このリレー１７は、出力ユニット９Ａ，９Ｂの出力値が動作方向で一致した場合のみ動作するようになっている。

【００３３】共有メモリ１６Ａ，１６Ｂには、それぞれ自系の入力データや出力データ等が記憶されるようになっている。しかし、Ｉ／Ｏバスコントローラ１５Ａ，１５Ｂの制御により、コントローラ１Ａ，１Ｂはそれぞれ自系の共有メモリの内容だけでなく、他系の共有メモリの内容についても読み取ることができるようになっている。

【００３４】ヘルシー回路１０Ａは、自系が正常な状態であるか否かを示す信号を出力する回路である。正常な状態の場合は、出力回路１１Ａからの交番信号がトランス１２Ａを介してリレー１３Ａを励磁し、ヘルシーリレー接点１４Ａがオン状態となる。一方、故障状態の場合は、ヘルシーリレー接点１４Ａはオフとなる。ヘルシーリレー接点１４Ａがオフとなっている場合は、もちろんＡ系は制御を停止しているが、ヘルシーリレー接点１４Ａがオフになるとヘルシーリレー接点１４Ｂもオフとなり、Ｂ系も結局制御を停止するようになっている。

【００３５】上記した図１の構成は、コントローラ部分が他の部分とＩ／Ｏインタフェイスで分離されており、独立性が強いものとなっている。したがって、汎用性の高いボードコンピュータ等を採用することができ、マイクロプロセッサのみを高機能の機種と交換することによって、機能の向上や新機種への対応を容易に図ることが可能な構成となっている。

【００３６】図２は、図１における入力ユニット８Ａ，８Ｂの構成と、この入力ユニット８Ａ，８Ｂとの間で信号の授受を行うマイクロプロセッサ・コントローラ１Ａ，１Ｂの構成とを示すブロック図である。この図において、入力ユニット８Ａは、抵抗１９Ａと、発光ダイオード２１Ａ及びフォトトランジスタ２２Ａにより形成されるフォトカプラ２０Ａ（入力用半導体素子）と、発光ダイオード２４Ａ及びフォトトランジスタ２５Ａにより形成されるフォトカプラ２３Ａ（チェック用半導体素子）とを有している。

【００３７】コントローラ１Ａは、故障診断回路２６Ａと、信号入力回路２７Ａと、比較照合回路２８Ａと、チェック信号発生回路２９Ａとを有している。そして、入力ユニット８Ｂ及びコントローラ１Ｂも入力ユニット８Ａ及びコントローラ１Ａと同様の構成を有している。

【００３８】入力ユニット８Ａ，８Ｂには入力接点信号Ｓ1が入力されるようになっている。入力接点信号Ｓ1は、踏切付近の所定区間内に列車が存在するか否かを知

らせる２値信号であり、“０”は列車が存在する場合、“１”は列車が存在しない場合を示している。ここで、入力ユニット８Ａ，８Ｂのフェイルセーフ機能について説明すると、信号Ｓ1の入力の際のフェイルセーフ性とは、信号“０”を誤って信号“１”と判別してしまうことを確実に防止することをいう。

【００３９】すなわち、入力ユニットに何らかの故障が生じ、実際の入力信号“０”（列車が存在する）を入力信号“１”（列車が存在しない）と誤って認識して遮断機を開放した場合には重大事故に直結する虞れがあるので、このような故障は絶対に回避しなければならない。このような故障を「危険側故障」と呼ぶ。これに対し、実際の入力信号“１”（列車が存在しない）を入力信号“０”（列車が存在する）と誤って認識させるような故障は直ちに重大事故に直結するものではないため、このような故障を「安全側故障」と呼ぶ。図２の構成は、上記の危険側故障に起因する事故を確実に防止するためのものである。

【００４０】次に、図２の動作につき説明する。まず、入力ユニット８Ａ，８Ｂのいずれにも故障が生じていない場合を考える。例えば、入力接点信号Ｓ1として信号“０”が入力ユニット８Ａ，８Ｂに入力されると、入力ユニット８Ａ内の抵抗１９Ａ、発光ダイオード２１Ａ、フォトトランジスタ２５Ａの経路には電流が流れないので、コントローラ１Ａ内の信号入力回路２７Ａも“０”を入力する。この入力結果は共有メモリ１６に書き込まれる。入力ユニット８Ｂ及びコントローラ１Ｂ内でも同様の動作が行われる。

【００４１】比較照合回路２８Ａは、共有メモリ１６に書き込まれている信号入力回路２７Ｂの入力結果を読み出し、これと信号入力回路２７Ａの入力結果との比較照合を行う。この照合結果は故障診断回路２６Ａに送られ、これに基づき故障診断回路２６Ａは故障診断を行う。コントローラ１Ｂ内の比較照合回路２８Ｂ及び故障診断回路２６Ｂも同様の動作を行う。この場合は、比較照合回路２８Ａ，２８Ｂの照合結果は一致し、従って故障診断回路２６Ａ，２６Ｂはいずれも正常である旨の診断を行う。

【００４２】ところが、入力ユニット８Ａ内のフォトトランジスタ２２Ａが導通故障している場合、実際の入力接点信号Ｓ1は“０”にも拘わらず信号入力回路２７Ａは“１”を入力することになる。この場合のフォトトランジスタ２２Ａの導通故障は危険側故障であるが、図２の構成によればこのような故障に基づく入力結果を排除することができる。

【００４３】すなわち、チェック信号発生回路２９Ａは、チェック信号としての“０”信号及び“１”信号を定期的に交互に出力している。いま、チェック信号発生回路２９Ａが“０”信号を発光ダイオード２４Ａに出力している状態であればフォトトランジスタ２５Ａはオフ状態であるため、発光ダイオード２１Ａには電流が流れず、従ってフォトトランジスタ２２Ａも必ずオフ状態となるはずである。それにもかかわらず、信号入力回路２７Ａが“１”を入力しているのはフォトトランジスタ２２Ａに導通故障が生じていることに他ならない。故障診断回路２６Ａは、このチェック信号発生回路２９Ａの出力状態と信号入力回路２７Ａの入力結果とに基づいて入力ユニット８Ａが故障であると判断する。

【００４４】一方、チェック信号発生回路２９Ａが“１”信号を出力している状態の場合は、信号入力回路２７Ａが“１”を入力したとしてもそれだけでは入力ユニット８Ａに故障が生じているか否かは分からない。しかし、この場合、比較照合回路２８ＡがＢ系との間で照合を行っているので、故障診断回路２６Ａはこの照合結果によって入力ユニット８Ａに故障が生じていることを判断することができる。

【００４５】また、入力接点信号Ｓ1が“０”である状態でフォトトランジスタ２２Ａにオープン故障が生じる場合がある。この場合は、チェック信号発生回路２９Ａの出力信号が“０”又は“１”のいずれであっても信号入力回路２７Ａは“０”を入力し、正常状態における場合と同様の入力結果を示すため、故障診断回路２６Ａは正常と判断することになる。つまり、コントローラ１Ａは正常と判断しているが実際には故障が潜在した状態となっている。しかし、この故障は既述したように安全側故障であり、直ちに検出されなくても重大事故に直結するものではないため許容され得る看過である。

【００４６】図３は、入力ユニットの代表的な故障モードを示した図表である。上述した例は、項目１乃至４に該当する。なお、“０”信号及びこれに続く“１”信号を１組の信号と見た場合には、一見すると、項目１及び項目２、あるいは項目３及び項目４を一つの項目として表記することも可能であるように思える。しかし、入力ユニットの正常・故障状態は瞬時に変化する可能性を有することから、フェイルセーフ機能を追求するためには、チェック信号発生回路２９Ａが“０”信号を出力した時点及び“１”信号を出力した時点の各時点において単独で正常又は故障の判断を行う必要がある。それ故、図３においては、項目１，２、項目３，４、　…　項目１９，２０等をそれぞれまとめて表記せず、単独の項目として表記しいている。

【００４７】図４は、図１における出力ユニット９Ａ，９Ｂの構成と、この出力ユニット９Ａ，９Ｂとの間で信号の授受を行うマイクロプロセッサ・コントローラ１Ａ，１Ｂの構成とを示すブロック図である。この図において、出力ユニット９Ａは、発光ダイオード３１Ａ及びフォトトランジスタ３２Ａにより形成されるフォトカプラ３０Ａ（出力用半導体素子）と、発光ダイオード３４Ａ及びフォトトランジスタ３５Ａにより形成されるフォトカプラ３３Ａ（故障検出用半導体素子）と、発光ダイ

オード３７Ａ及びフォトトランジスタ３８Ａにより形成されるフォトカプラ３６Ａ（チェック用半導体素子）と、抵抗３９Ａとを有している。出力ユニット９Ｂも出力ユニット９Ａと同様の構成を有しているが、その他に、ダイオード４０及び抵抗４１を有している。

【００４８】コントローラ１Ａは、出力信号駆動回路４２Ａと、故障検出回路４３Ａと、チェック信号発生回路４４Ａと、接点リードバック回路４５Ａとを有している。そして、コントローラ１Ｂもコントローラ１Ａと同様の構成を有している。また、図１においても示したリレー１７及びリレー接点１８は、遮断機制御装置などの現場機器内に配設されている。

【００４９】２４ボルト電源の高圧側端子には直列接続されたヘルシーリレー接点１４Ａ，１４Ｂを介してフォトカプラ３０Ａが接続されており、これに続いてフォトカプラ３０Ｂ、ダイオード４０を介してリレー１７の一端側が接続され、リレー１７の他端側が２４ボルト電源の０ボルト端子に接続されている。したがって、出力ユニット９Ａの信号出力経路と、出力ユニット９Ｂの信号出力経路とは互いに直列接続されている。

【００５０】リレー１７に対して励磁信号としての“１”信号が出力ユニット９Ａ及び９Ｂから同時に出力されてリレー１７が励磁されている状態では、リレー接点１８が閉じ、遮断機が上がった状態となっている。また、リレー１７に対して無励磁信号としての“０”信号が出力ユニット９Ａ及び９Ｂから出力されてリレー１７が無励磁の状態になっていれば、リレー接点１８が開き、遮断機が下がった状態になっている。したがって、出力ユニットのフェイルセーフ性とは、“０”信号を出力して遮断機を下げていなければならない場合にもかかわらず、誤って“１”信号が出力され遮断機を上げてしまうような故障を確実に防止することである。図４の出力ユニットの構成は、図２の入力ユニットの場合と同様に、“１”信号を危険側信号、“０”信号を安全側信号として扱い、危険側故障に起因する事故を確実に防止するためのものである。

【００５１】次に、図４の動作につき説明する。Ａ系及びＢ系のいずれも正常に機能している場合はヘルシーリレー接点１４Ａ，１４Ｂの双方がオンになっている。いま、出力信号駆動回路４２Ａ，４２Ｂの一方又は双方から“０”信号が出力されていれば、フォトトランジスタ３２Ａ，３２Ｂ及びダイオード４０の経路には電流が流れないので、リレー１７は無励磁状態であり、したがって遮断機は下がった状態となっている。このとき、リレー接点１８はオフとなっており、接点リードバック回路４５Ａ，４５Ｂは“１”信号を検出する。一方、出力信号駆動回路４２Ａ，４２Ｂの双方から“１”信号が出力されていれば、フォトトランジスタ３２Ａ，３２Ｂ及びダイオード４０の経路に電流が流れるので、リレー１７は励磁状態となり、したがって遮断機は上がった状態となる。このとき、リレー接点１８はオンとなり、接点リードバック回路４５Ａ，４５Ｂは“０”信号を検出する。

【００５２】そして、上記のように、フォトトランジスタ３２Ａ，３２Ｂ及びダイオード４０の経路に電流が流れていない状態では、抵抗３９Ａ，発光ダイオード３４Ａ側及び抵抗３９Ｂ，発光ダイオード３４Ｂ側にそれぞれ微弱電流が流れ、故障検出回路４３Ａ，４３Ｂが“１”信号を入力するようになっている。一方、フォトトランジスタ３２Ａ，３２Ｂ及びダイオード４０の経路に電流が流れている状態では、抵抗３９Ａ，発光ダイオード３４Ａ側及び抵抗３９Ｂ，発光ダイオード３４Ｂ側に微弱電流は流れず、故障検出回路４３Ａ，４３Ｂは“０”信号を入力するようになっている。

【００５３】上記の故障検出回路４３Ａ，４３Ｂによりフォトトランジスタ３２Ａ，３２Ｂの故障を検出することができる。すなわち、例えば、フォトトランジスタ３２Ａが導通故障している場合には、出力信号駆動回路４２Ａから“０”信号が出力されているにもかかわらず、故障検出回路４３Ａが“０”信号を入力する（正常であれば、回路４３Ａは“１”信号を入力するはずである。）。したがって、フォトトランジスタ３２Ａの導通故障を検出することができる。また、フォトトランジスタ３２Ａがオープン故障している場合には、出力信号駆動回路４２Ａから“１”信号が出力されているにもかかわらず、故障検出回路４３Ａが“１”信号を入力する（正常であれば、回路４３Ａは“０”信号を入力するはずである。）。したがって、フォトトランジスタ３２Ａのオープン故障を検出することができる。

【００５４】上記のように、フォトカプラ３３Ａ及び故障検出回路４３Ａによりフォトトランジスタ３２Ａの故障を検出することができるようになっている。しかし、フォトカプラ３３Ａのフォトトランジスタ３５Ａが故障した場合、特に、その故障が導通故障である場合はフェイルセーフ性を維持することができなくなる。なぜなら、フォトトランジスタ３５Ａが導通故障している場合は故障検出回路４３Ａの入力が常時“１”となるため、フォトトランジスタ３２Ａに導通故障が生じ、危険側信号である“１”信号が誤ってリレー１７に出力されても、これを検出することができなくなるからである（これに対し、フォトトランジスタ３５Ａのオープン故障の場合は、故障検出回路４３Ａの入力が常時“０”となり、コントローラ自体がリレー１７に危険側信号である“１”信号が出力されていることを認識していることになるので重大事故に直結することはない。）。したがって、フェイルセーフ性を確保するためには、フォトトランジスタ３５Ａの導通故障は確実に検出すべき事象である。フォトカプラ３６Ａ及びチェック信号発生回路４４Ａは、この確実に検出すべき事象であるフォトトランジスタ３５Ａの導通故障を検出するために設けられたもの

であり、チェック信号発生回路４４Ａは定期的に“０”信号及び“１”信号を交互に出力している。

【００５５】すなわち、チェック信号発生回路４４Ａはチェック信号としての“１”信号及び“０”信号を交互に発光ダイオード３７Ａに出力し、フォトトランジスタ３８Ａをオンオフする。これにより、発光ダイオード３４Ａに流れる電流が強制的にオンオフされる。したがって、故障検出回路４３Ａが“１”信号を入力した状態でチェック信号発生回路４４Ａがチェック信号を出力した場合に、このチェック信号に応じて故障検出回路４３Ａの信号入力状態が変化せず、連続して“１”信号を入力している状態となっているのであれば、それはフォトトランジスタ３５Ａに導通故障が発生しているからであるということが分かる。

【００５６】図５は、出力信号駆動回路４２Ａ、接点リードバック回路４５Ａ、チェック信号発生回路４４Ａ、及び故障検出回路４３Ａの動作を説明するためのタイムチャートであり、（ａ）は正常動作の場合、（ｂ）は危険側故障の場合、（ｃ）は安全側故障の場合をそれぞれ示している。なお、「出力されるべき信号」とは、リレー１７に対して本来正しく出力されるべき信号の意味である。

【００５７】図５（ａ）に示されるように、正常の場合には、故障検出回路４３Ａが入力する信号は、チェック信号発生回路４４Ａが“０”信号を出力している場合には必ず“０”であり、また、チェック信号発生回路４４Ａが“１”信号を出力している場合には接点リードバック回路４５Ａが読み取った信号と同じ信号となっている。

【００５８】しかし、図５（ｂ）に示されるように、フォトトランジスタ３５Ａに導通故障が生じた場合は、チェック信号が“０”であるにもかかわらず故障検出回路４３Ａは“１”信号を入力している。そのため、この時点で直ちにシステムを停止させて危険側故障に起因する重大事故の発生を未然に防止するようにしている。もし、この時点でシステムを停止させずにそのまま運転を継続した場合、フォトトランジスタ３２Ａに導通故障が生じても、これを検出することができなくなるからである。

【００５９】また、図５（ｃ）に示されるように、フォトトランジスタ３５Ａにオープン故障が生じた場合は、接点リードバック回路４５Ａが“０”信号を読み取っている期間は、チェック信号の変化によってもこのオープン故障は検出されることがない。しかし、既述した通り、この期間中にフォトトランジスタ３５Ａのオープン故障が検出できなくとも重大事故に直結することはない。そして、この状態のままフォトトランジスタ３２Ａにオープン故障が発生すると、チェック信号が“１”であるにもかかわらず故障検出回路４３Ａが入力する信号が“０”となり、接点リードバック回路４５Ａの信号と一致しないために、フォトトランジスタ３２Ａのオープン故障が検出され、システムが停止されることになる。図６に、上述したような故障を含めた、出力ユニットの代表的な故障モードを示す。

【００６０】ところで、図４におけるフォトトランジスタ３２Ａ，３２Ｂは特異な状態に陥る可能性を有するものである。特異な状態とは、例えば、出力信号駆動回路４２Ａが“０”信号を出力している場合に、フォトトランジスタ３２Ａが不飽和の状態でその漏れ電流を増加させ、リレー１７を励磁してしまう虞れのあるレベルの電流を流している状態のことをいう（この状態のことを「半導通状態」と呼ぶ。）。この半導通状態では、リレー１７は実際には励磁されておらず、故障検出回路４３Ａも“１”信号を入力しているので何らの故障も検出されていない。しかし、フォトトランジスタ３２Ａがこのような半導通状態に陥っている間にフォトトランジスタ３２Ｂに導通故障が生じると、出力信号駆動回路４２Ａ，４２Ｂが“０”信号を出力しているにもかかわらずリレー１７が励磁されてしまい、出力ユニット９Ａ，９Ｂのフェイルセーフ性が失われることになる。重大事故の発生を確実に防ぎ安全性を向上させるためには、このような半導通状態が生じていることを確実に検出し、速やかにシステムを停止させてフェイルセーフ性を維持することが求められる。図４の構成によれば、このような半導通状態を確実に検出することが可能である。

【００６１】すなわち、正常の状態において出力信号駆動回路４２Ａが“０”信号を出力している場合には、微弱電流が抵抗３９Ａ、発光ダイオード３４Ａ、フォトトランジスタ３８Ａを通って出力ユニット９Ｂ側に出力されるが、この出力される微弱電流はチェック信号発生回路４４Ａの働きによって“０”と“１”とが交互に繰り返される信号となっている。したがって、チェック信号発生回路４４Ｂの出力によりフォトトランジスタ３８Ｂがオンになっている状態において、故障検出回路４３Ｂは、出力ユニット９Ａ側からの信号が“１”の場合には“１”信号を入力し、出力ユニット９Ａ側からの信号が“０”の場合には“０”信号を入力するはずである。ところが、フォトトランジスタ３２Ａが上記の半導通状態に陥っている場合には、その漏れ電流によって出力ユニット９Ａからの電流レベルが上昇し、故障検出回路４３Ｂは、フォトトランジスタ３８Ｂがオンになっている状態においては常時“１”信号を入力することになる。この現象により、フォトトランジスタ３２Ａが半導通状態にあることを検出することができる。上記の例は、Ａ系側のフォトトランジスタ３２Ａが半導通状態にあることをＢ系側の故障検出回路４３Ｂの入力状態に基づいて判別していたが、Ｂ系側のフォトトランジスタ３２Ｂに半導通状態が生じている場合もＡ系側の故障検出回路４３Ａの入力状態に基づいて判別することができる。

【００６２】次に、図１において示したヘルシー回路１

０Ａ，１０Ｂにつき説明する。図７は、このヘルシー回路１０Ａ，１０Ｂの構成図である。図７においてＡ系を例に取り説明すると、コントローラ１Ａのマイクロプロセッサ・ユニット２Ａは交番信号を生成するが、この交番信号は入出力インタフェイス５Ａ及びＩ／Ｏバス７Ａを介してヘルシー回路１０Ａに送出される。そして、ヘルシー回路１０Ａでは、出力回路１１Ａがこの交番信号をトランス１２Ａの１次側に出力し、その２次側からは直流分がカットされて交番信号の交流分のみが出力される。トランス１２Ａの２次側から出力される交番信号はダイオード４６Ａにより整流され、この整流された電流によってリレー１３Ａが励磁され、ヘルシーリレー接点１４Ａがオンとなる。

【００６３】上記したように、リレー１３Ａは間接的にはマイクロプロセッサ・ユニット２Ａによって生成される交番信号に基づき励磁されるので、マイクロプロセッサ・ユニット２Ａが故障を検知した場合には必ず無励磁となってヘルシーリレー接点１４Ａがオフとなる。つまり、マイクロプロセッサ・ユニット２Ａが故障を検知した場合、通常、マイクロプロセッサ・ユニット２Ａは全ての出力をクリアして“０”とするが、故障の種類によっては出力をクリアできなくなることがある。そして、マイクロプロセッサ・ユニット２Ａから出力回路１１Ａに対して“１”信号が出力され続けることになるが、この場合には出力回路１１Ａがトランス１２Ａの１次側に供給する信号が交番信号ではなくなり、トランス１２Ａの２次側出力はゼロとなるためリレー１３Ａが励磁されることはない。したがって、マイクロプロセッサ・ユニット２Ａが故障を検知した場合にはリレー１３Ａは必ず無励磁となってヘルシーリレー接点１４Ａをオフの状態にすることができる。そして、図４において図示したように、ヘルシーリレー接点１４Ａ，１４Ｂは直列接続された状態で電源回路に接続されているので、いずれか一方がオフになった場合には決して現場機器内のリレー１７が励磁されることがない。

【００６４】図８は、出力回路１１Ａ，１１Ｂの信号出力状態とリレー１３Ａ，１３Ｂの励磁状態を示すタイムチャートである。この図において、当初Ａ系及びＢ系共に正常に機能していたが、ある時点でＡ系のマイクロプロセッサ・ユニット２Ａが故障を検知したとする。すると、マイクロプロセッサ・ユニット２Ａは直ちに全ての出力をクリアするため出力回路１１Ａからの交番信号の出力は停止され、それまで励磁状態となっていたリレー１３Ａは無励磁状態となる。そして、Ｂ系のマイクロプロセッサ・ユニット２Ｂは、Ａ系のマイクロプロセッサ・ユニット２Ａが交番信号の生成を停止したことを照合機能によって検知できるようになっている。したがって、マイクロプロセッサ・ユニット２Ｂも、この後すぐに交番信号の生成を停止する。これにより、出力回路１１Ｂからの交番信号の出力も停止されリレー１３Ｂも無励磁状態となる。

【００６５】ここで、上記の交番信号において“１”となっている時間及び“０”となっている時間を一定に保つための技術につき説明する。交番信号を出力する場合、通常は、マイクロプロセッサ・ユニット２Ａがメインプログラムで出力することが考えられる。しかし、マイクロプロセッサ・ユニット２Ａの処理が正常に行われている間はメインプログラムの制御処理時間が一定であるため特に問題は生じないが、外部からの入力信号の入力状況如何によってはこの制御処理時間が一定でなくなり、“１”である時間及び“０”である時間を一定に保つことが困難になる。

【００６６】そこで、本実施形態では、図９に示すように、マイクロプロセッサ・ユニット２Ａ内にメインプログラムを実行する制御処理手段４７の他に、割り込みプログラムを実行する交番信号発生手段４８を設け、これにより交番信号を発生させるようにしている。制御処理手段４７はカウンタ４９及び走行フラグ５０を有しており、交番信号発生手段４８はカウンタ５１を有している。

【００６７】このような構成によりフェイルセーフな交番信号を発生させるためには、メインプログラムに異常が生じた場合は、割込プログラムによって確実にその走行を停止させて交番信号の発生を停止させる必要がある。一方、割込プログラムに異常が生じた場合も、メインプログラムによって確実にその走行を停止させて交番信号の発生を停止させる必要がある。そして、交番信号の周期はできるだけ短い方が望ましいが、割込プログラムが余りに頻繁に走行するとメインプログラムでの処理時間がなくなってしまうので、その周期は適切に選ぶ必要がある。図９の例では、制御処理手段４７が実行するメインプログラムの１回の処理時間を１００～２００ｍｓとし、交番信号発生手段４８が実行する割込プログラムの割込周期を５ｍｓとする。したがって、正常状態であれば、メインプログラムの１回の処理時間の間に割込プログラムが２０～４０回走行することになる。この関係を利用してヘルシー回路の交番信号を発生させることができる。

【００６８】次に、図９の動作につき説明する。なお、この例では、メインプログラムの１回の処理時間を１００ｍｓとし、正常な割込回数を２０±１回とする。制御処理手段４７は、１回の走行開始時に走行フラグ５０をセットすると共にカウンタ４９に走行回数についてのカウント値を加算し、更に１回の走行終了時に走行フラグ５０をリセットする。一方、交番信号発生手段４８は、走行フラグ５０がセットされると５ｍｓ毎の割込を走行フラグ５０がリセットされるまで行い、“１”又は“０”の交番信号を発生させる。そして、交番信号発生手段４８は、このときの割込回数についてのカウント値をカウンタ５１に加算する。

【００６９】制御処理手段４７が１回の走行を終了して走行フラグ５０をリセットし、次の走行を行うべく再度走行フラグ５０のセットを行うと、この時点で交番信号発生手段４８は、カウンタ５１のカウント値をチェックする。いま、カウンタ５１のカウント値が２２回であったとすると、制御処理手段４７は、メインプログラムに異常が発生していると判別し、全プログラムの走行を停止させる。

【００７０】一方、制御処理手段４７の側でもこの時点でカウンタ５１のカウント値をチェックしている。したがって、交番信号発生手段４８側に何らかの異常が発生し、その結果カウンタ５１のカウント値が２２回になった場合であっても、制御処理手段４７は、割込異常として全プログラムの走行を停止させることができる。

【００７１】なお、制御処理手段４７は、上記の割込異常以外の異常（例えば、Ｂ系側の入力データとの照合結果が一致しない等の異常）が生じた場合は、図示を省略してあるエラーフラグをセットして全プログラムを停止させる。このエラーフラグについては、交番信号発生手段４８もチェックしており、エラーフラグがセットされると直ちに割込プログラムの走行を停止し、交番信号の発生を停止するようになっている。

【００７２】上記した図９の構成によれば、メインプログラム側が何らかの原因で処理時間がかかる故障を起こした場合、あるいは処理時間が余りに短いような故障を起こした場合に、メインプログラム自身がこれらの故障を検出できないときでも、割込プログラムにより故障を検出してヘルシーリレーを無励磁にすることができる。また、割込プログラム側が割込頻度が異常に高い故障又は異常に低い故障を起こした場合は、これをメインプログラムで検出してヘルシーリレーを無励磁にすることができる。すなわち、高速で且つ高精度の周期を有する交番信号を出力することができ、フェイルセーフを実現することができる。さらに、交番信号を高速化することができるため、ヘルシー回路１０Ａ，１０Ｂ内のトランス１２Ａ，１２Ｂを小型化することができ、速い応答性を得ることができるようになる。

【００７３】次に、図１に示した共有メモリ１６Ａ，１６Ｂの利用により、プログラムの内容の一部を効率的に書き換える技術につき説明する。一般に、電子踏切制御装置のプログラムには標準的なものが用意されているが、タイマ等の定数については現場の踏切の実際の状況に合わせる必要があるため、予めインストールされているプログラムの内容の一部を変更して使用する場合が通常である。このようなプログラム内容の変更は、電子踏切制御装置を実際に設置する際や、設置後の運用結果に基づいて行われることが多いが、いずれにしても現場において行わなければならないので、この変更処理は容易且つ確実に実行できるようにしておくことが望ましい。本実施形態の構成によれば、共有メモリの働きにより、Ａ系又はＢ系のいずれか一方の系のみに対してプログラム内容の一部を変更すれば、他方の系のプログラム内容も自動的に変更されるようにすることができる。

【００７４】すなわち、現場にいるオペレータは、図１においては図示を省略してあるＰＣ（パーソナル・コンピュータ）モニタを操作して、変更すべきタイマ等の定数をマイクロプロセッサ・ユニット２Ａを介して記憶部３Ａに書き込む。この記憶部３Ａは、既述したように、ＥＥＰＲＯＭにより形成されているので、電気的な書込が可能であり、また、電源が停電した場合でもデータ保持が可能なものである。

【００７５】記憶部３Ａに書き込まれたデータは共有メモリ１６Ａにも書き込まれるが、Ｂ系マイクロプロセッサ・コントローラ１Ｂはこの共有メモリ１６Ａの内容を読み出し、これを自系の記憶部３Ｂ及び共有メモリ１６Ｂに書き込む。そして、Ａ系マイクロプロセッサ・コントローラ１Ａは、共有メモリ１６Ａのデータと共有メモリ１６Ｂとを照合し、その照合結果をＰＣモニタに出力する。ＰＣモニタは、Ａ系に書き込まれたデータと、Ａ系への書込に伴ってＢ系に書き込まれたデータとを比較し、両者が一致していれば正常である旨を表示し、また、不一致であればＡ系の動作を停止するようにＡ系マイクロプロセッサ・コントローラ１Ａに指示する。なお、変更データの信頼性を高めるために、定数データにはデータの誤りを検出できるチェックコードを一緒に送信することも可能である。

【００７６】このように、図１の構成によれば、タイマ等の定数などを変更する場合、２台のマイクロプロセッサ・コントローラのうち１台のみに対して変更処理を行えば、他方の系の定数も自動的に変更される。そして、自系と他系の変更内容が同一になっているか否かについてのチェックも同時に実行することができるので、人間の操作ミスによる誤った定数の設定を防止することができる。

【００７７】次に、本発明の第２の実施形態につき説明する。図１０はこの第２の実施形態の構成を示すブロック図である。図１に示した第１の実施形態は、Ａ系（第１の制御系）及びＢ系（第２の制御系）の２つの制御系を有するものであったが、この第２の実施形態は３つの制御系を有するものであり、Ａ系及びＢ系の２つの制御系の他にさらにＣ系（第３の制御系）を有するものである。そして、図１１は、この図１０に示した電子踏切制御装置を用いて構成した電子踏切制御システムの構成図である。

【００７８】まず、図１１の電子踏切制御システムについて先に説明する。この図において、第１の制御処理端末装置６１、第２の制御処理端末装置６２、及び４台の入出力処理端末装置６３～６６の各制御系は、Ａ～Ｃ系のＬＡＮによって互いに接続されている。そして、入出力処理端末装置６３～６６は、それぞれ現場機器６７～

７０との間で信号の授受を行うようになっている。

【００７９】第１の制御処理端末装置６１及び第２の制御処理端末装置６２は入出力処理端末装置６３～６６の上位機器であり、現場機器６７～７０は実質的にはこれら第１の制御処理端末装置６１又は第２の制御処理端末装置６２により、入出力処理端末装置６３～６６を介して制御されることになる。

【００８０】第１の制御処理端末装置６１には現在の列車運行に用いられるプログラムが実装されており、第２の制御処理端末装置６２には新しく開発された応用プログラムが実装されている。そして、列車運行数が多い時間帯（昼間）には全ての現場機器６７～７０が稼働するが、列車運行数が少ない時間帯（夜間）には現場機器６７のみが稼働し、現場機器６８～７０に対しては改修工事あるいは試験等が行われるものとする。

【００８１】入出力処理端末装置６３～６６のそれぞれは、第１の制御処理端末装置６１又は第２の制御処理端末装置６２のうちのいずれと信号の授受を行うかを決める切換スイッチを有しており、この切換スイッチの制御は第２の制御処理端末装置６２により行われるようになっている。昼間は、全ての入出力処理端末装置６３～６６は現場機器６７～７０からの入力信号を第１の制御処理端末装置６１のみに対して出力し、一方、第１の制御処理端末装置６１のみが入出力処理端末装置６３～６６に対して信号を出力する。しかし、夜間になって第２の制御処理端末装置６２が上記の切換スイッチを所定の位置に切り換えると、入出力処理端末装置６３のみが現場機器６７からの入力信号を第１の制御処理端末装置６１に対して出力し、一方、第１の制御処理端末装置６１は入出力処理端末装置６３のみに対して信号を出力する。そして、入出力処理端末装置６４～６６は、現場機器６８～７０からの入力信号を第２の制御処理端末装置６２に対して出力し、一方、第２の制御処理端末装置６２は入出力処理端末装置６４～６６に対して信号を出力する。

【００８２】このような鉄道用保安制御システムによれば、特定の線路を使用する列車の運行は継続したままで、他の線路に設けられた踏切の改修工事あるいは試験等を行うことが可能になるので、改修工事の効率を大きく向上させることができ、工期の短縮を図ることができる。

【００８３】次に、図１０の構成につき説明する。この図において、Ａ系のマイクロプロセッサ・コントローラ７１Ａは、マイクロプロセッサ・ユニット７２Ａ、メモリ部７３Ａ、ＬＡＮ制御部７４Ａ、及びＩ／Ｏバス・インタフェイス７５Ａを有している。マイクロプロセッサ・コントローラ７１ＡはＩ／Ｏバス・インタフェイス７６Ａを介して入力ユニット７７Ａ、出力ユニット７８Ａ、及びヘルシー回路７９Ａと接続されている（入力ユニット７７Ａ及び出力ユニット７８Ａ構成は、それぞれ図２及び図４に示したものと略同様の構成のものである。）。Ｂ系及びＣ系もＡ系と同様の構成を有している。そして、Ａ系とＢ系との間には共有メモリ８０、Ｂ系とＣ系との間には共有メモリ８１、Ｃ系とＡ系との間には共有メモリ８２が、それぞれ設けられている。

【００８４】各系の入力ユニット７７Ａ，７７Ｂ，７７Ｃには、現場機器入力信号モジュール８３を介して現場機器６７（又は現場機器６８～７０）からの信号が入力されるようになっており、また、各系の出力ユニット７８Ａ，７８Ｂ，７８Ｃからの信号が現場機器出力信号モジュール８４を介して現場機器６７に出力されるようになっている。そして、各系のヘルシー回路７９Ａ，７９Ｂ，７９Ｃからのヘルシーリレー接点信号の状態が、現場機器出力信号モジュール８４、さらに現場機器入力信号モジュール８３に対して送出されるようになっており、３系のうち少なくとも２系が正常でなければ現場機器出力信号モジュール８４及び現場機器入力信号モジュール８３が動作しないようになっている。なお、現場機器入力信号モジュール８３及び現場機器出力信号モジュール８４は、図１０の構成についての理解を容易にするために概念的な要素として図示したものであり、実際には各コントローラ内のマイクロプロセッサ・ユニット７２Ａ，７２Ｂ，７２Ｃの機能として考えられるものである。

【００８５】図１２は、図１０におけるヘルシー回路７９Ａ，７９Ｂ，７９Ｃの構成図である（ヘルシー回路７９Ｂ，７９Ｃの構成はヘルシー回路７９Ａと同様であるため省略する。）。この図において、Ａ系マイクロプロセッサ・コントローラ７１Ａのマイクロプロセッサ・ユニット７２Ａは交番信号を生成するが、この交番信号はＩ／Ｏバス・インタフェイス７５Ａ，７６Ａを介してヘルシー回路７９Ａに送出される。ヘルシー回路７９Ａでは、２つの出力回路８５Ａ1，８５Ａ2がこの交番信号をそれぞれトランス８６Ａ1，８６Ａ2の１次側に出力し、その２次側からは直流分がカットされて交番信号の交流分のみが出力される。トランス８６Ａ1，８６Ａ2の各２次側から出力される交番信号はそれぞれダイオード８７Ａ1，８７Ａ2により整流され、この整流された電流によってリレー８８Ａ1，８８Ａ2が励磁され、ヘルシーリレー接点８９Ａ1，８９Ａ2がオンとなる。

【００８６】図１２のヘルシー回路７９Ａの動作は、図７の場合と略同様であるため、その重複した説明は省略し、各系の間のヘルシーリレー接点のオンオフの組合せのみについて説明する。図１２における「ヘルシーＡ＝Ｂ，ヘルシーＡ＝Ｃ，…ヘルシーＣ＝Ｂ」は、他系と関連するヘルシーリレー接点を示している。つまり、イコール記号の左側のアルファベット記号は自系側を示し、イコール記号の右側のアルファベット記号は他系側を示している。

【００８７】そして、例えば、Ａ系コントローラが自己

診断によって自系の故障を検出した場合は、A＝B及びA＝Cの接点をオフにして自系の走行を停止する。このとき、B系側ではB＝Cの接点はオンのままにしておくが、A系と関連する接点であるB＝Aの接点をオフにする。同様に、C系側でもC＝Bの接点はオンのままにしておくが、A系と関連する接点であるC＝Aの接点をオフにする。

【００８８】一方、A系コントローラがその照合機能によって他系の故障を検出した場合は、その他系と関連する接点のみをオフにする。例えば、A系コントローラがB系の故障を検出した場合は、A＝Bの接点のみをオフにしてA＝Cの接点はオンにしておく。このとき、C系側でもC系コントローラがB系の故障を検出し、C＝Bの接点のみをオフにしてC＝Aの接点はオンにしてあるはずである。そして、A系側及びC系側の各接点A＝B及びC＝Bがオフになったことにより、B系側の接点B＝C及びB＝Aもオフとなり、B系の走行が停止される。

【００８９】図１０に示した第２の実施形態は、既述したように、A系，B系，C系の３重系構成を有するものであり、そのうち２系の入力データ又は出力データが一致した場合に、その入力データ又は出力データを正常データとして取り扱うとする、所謂「２out of３」方式を採用している。３系のうち２系の入出力データが一致する場合の態様としては、次の３つの態様がある。

【００９０】（１）A系及びB系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状態）であり、且つA系及びB系の出力データ（又は入力データ）が共に“１”である。

（２）B系及びC系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状態）であり、且つB系及びC系の出力データ（又は入力データ）が共に“１”である。

（３）C系及びA系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状であり、且つC系及びA系の出力データ（又は入力データ）が共に“１”である。

【００９１】例えば、B系において故障が発生した場合、ヘルシー回路７９Bの接点B＝C及びB＝Aがオフになると共に、ヘルシー回路７９A，７９Cの接点A＝B及びC＝Bがオフになる。しかし、ヘルシー回路７９A，７９Cの接点A＝C及びC＝Aはオン状態を維持しているので、正常なA系及びC系によってシステムの制御を継続することができる（上記の（３）の態様）。

【００９２】次に、図１０の動作を、図１３のフローチャートに基づき説明する。但し、図１３においてはA系及びB系相互間のみの動作を説明し、B系及びC系相互間並びにC系及びA系相互間についての重複した説明を省略する。

【００９３】コントローラ７１A，７１Bは、まず、プログラムで制御を開始するための同期処理を行う。すなわち、コントローラ７１A，７１Bは、「同期通番」と呼ばれる処理回数を示す番号を共有メモリ８０の自系領域８０A，８０Bに書き込み、自系の同期通番と他系の同期通番とが一致するか否かを確認することにより同期が取れたか否かを判別する（ステップ１０１A，１０１B）。同期が取れない場合は一定時間だけ待ち、それでも同期が取れない場合は互いに他系を故障と判断し、それぞれヘルシーリレー接点をオフにしてヘルシーリレーを無励磁とする。そして、同期が取れた場合は、そのタイミングで制御処理を開始する。

【００９４】同期が取れた後、各コントローラは、入力モジュール８３を通して入力した現場機器６７からの入力信号を読み込み、これを自系の記憶領域８０A，８０Bに書き込む。そして、自系に書き込んだ入力信号と他系に書き込まれた入力信号とが一致するか否かを判別する（ステップ１０２A，１０２B）。一致しない場合は、それぞれ他系を故障と判別し、一方、一致する場合は制御のための演算処理を行う（ステップ１０３A，１０３B）。

【００９５】各コントローラは、演算処理結果を出力信号として自系の記憶領域８０A，８０Bに書き込み、さらに自系に書き込んだ出力信号と他系に書き込まれた出力信号とが一致するか否かを判別する（ステップ１０４A，１０４B）。一致しない場合は、それぞれ他系を故障と判別し、一方、一致する場合は、これを出力モジュール８４を介して現場機器６７に出力する。

【００９６】このように、A系側コントローラは自系の制御処理を行うと共に、B系側コントローラに対する故障検出器としても機能しており、また、B系側コントローラも自系の制御処理を行うと共に、A系側コントローラに対する故障検出器としても機能している。したがって、現場機器との間で確実な入出力制御を行うことができる。

【００９７】図１４は、図１３において説明した他系との同期チェック処理、入力処理、及び出力処理を含め、エラー処理が行われる主な場合をA系側を例に取って示したフローチャートである。A系コントローラ７１Aは、まず、自系のＩ／Ｏバス等について異常がないか否かにつき自己診断を行い（ステップ１）、異常があった場合、すでに励振出力されていればエラー処理として励振処理の出力を停止し（ステップ１９）、制御動作を停止する（ステップ２０）。励振出力とは、図１２においてマイクロプロセッサ・ユニット７２Aが交番信号の発生し、出力回路８５A1，８５A2に交番信号を出力させることである。

【００９８】コントローラの自己診断の結果、異常がなければ上記の励振出力を行う（ステップ２）。そして、コントローラ７１Aは、共有メモリ８０，８２に対する書き込みテスト及び読み出しテストを行い（ステップ３）、異常があればステップ１９の処理を行う。次い

で、入力ユニット７７Ａ及び出力ユニット７８Ａのオフチェックを行って導通故障が生じていないかどうかをチェックし（ステップ４，５）、異常があればステップ１９の処理を行う。そして、前回の制御出力のリードバックを行い、異常がないか否かを確認する（ステップ６）。

【００９９】ステップ４～６のチェックの結果、異常がなければ、図１３において既述したように、他系すなわちＢ系及びＣ系との同期を取るようにし（ステップ７）、同期が取れなければステップ１９の処理を行う。同期が取れたならば、入力モジュール８３からデータを入力し入力処理を開始する（ステップ８）。そして、８ビットの反転データを作成して、これを共有メモリ８０，８２に書き込むと共に（ステップ９）、Ｂ系及びＣ系の反転データと照合することにより、これら他系と共有しているメモリデータのチェックを行い（ステップ１０）、異常があればステップ１９の処理を行う。次いで、入力モジュール８３から入力した入力信号について他系と一致するか否かを共有メモリ８０，８２を用いて照合し（ステップ１１）、異常があればステップ１９の処理を行う。

【０１００】上記の照合の後、２つの同一内容のプログラムである制御処理１，２をメモリエリアと時間を変えて実行する（ステップ１２，１３）。そして、制御処理１，２による演算結果を照合した結果（ステップ１４）、一致しなければ異常であるとしてステップ１９の処理を行う。

【０１０１】この後、この演算結果を出力しようとする前に、ステップ９，１０と同様に、反転データの作成及び書き込み並びに他系の反転データとの照合を行い（ステップ１５，１６）、異常があればステップ１９の処理を行う。次いで、出力モジュール８４から出力すべき出力信号について他系と一致するか否かを共有メモリ８０，８２を用いて照合し（ステップ１７）、異常があればステップ１９の処理を行う。そして、異常がなければ、出力処理を行い（ステップ１８）、ステップ１以下の動作を繰り返す。

【０１０２】Ａ系コントローラはステップ１９で励振出力を停止する場合において、自系の異常を検出したときは、Ａ＝Ｂ及びＡ＝Ｃの双方のヘルシーリレー接点をオフにし、Ｂ系（又はＣ系）の異常を検出したときは、Ａ＝Ｂのみ（又はＡ＝Ｃのみ）のヘルシーリレー接点をオフにする。そして、Ａ＝Ｂ及びＡ＝Ｃの双方のヘルシーリレー接点がオフになった場合、Ａ系コントローラは走行を停止するが（ステップ１９）、Ａ＝Ｂのみ（又はＡ＝Ｃのみ）のヘルシーリレー接点がオフになった場合は、Ｃ系（又はＢ系）との間で制御処理を続行する。

【０１０３】上述したように、３系のうちの１つの系に故障が発生した場合、その系のコントローラは自系のヘルシーリレーを無励磁にして自系の走行を停止させるようになっているが、もし、自系のヘルシーリレーを無励磁にできなかったとしても、他の２系が故障系のヘルシーリレーを無励磁にし、故障系を制御処理に参加させないようにしてシステムの安全性を確保している。しかし、故障系を除いた他の２系で制御処理を続行している間に、何らかの原因で故障系が再び制御処理に参加するような事態が生じるとシステムの安全性が阻害されることになる。そこで、本実施形態では、このような事態が生じることのないように、故障系の電源回路をオフにし、故障系を他の２つの健全な系から強制的に切断するようにしている。

【０１０４】図１５は、電源回路をオフにする系を各態様毎に示した図表である。なお、この電源回路は、図１０においては図示を省略してあるが、各系のコントローラ７１Ａ，７１Ｂ，７１Ｃ内に設けられているものである。図１５において、「０」は故障と判断された系又はその関連する系のヘルシーリレー接点（オフにされるべき接点）であり、「１」は正常な系のヘルシーリレー接点であることを示している。また、Ｘ1は故障のために既に電源回路がオフされている系のヘルシーリレー接点（当然、オフになっている）を示し、Ｘ2はＸ1に係るヘルシーリレー接点に追随してオフになっているヘルシーリレー接点を示している。

【０１０５】したがって、項目１は、３系で制御中にＡ系が故障したため、まずＡ系の接点Ａ＝Ｂ及びＡ＝Ｃをオフにすると共に、Ｂ系及びＣ系の接点Ｂ＝Ａ及びＣ＝Ａをオフにし、Ａ系の電源回路をオフにしてＢ系及びＣ系で制御処理を続行する場合を示している。項目２は、Ｃ系が故障のため既に電源回路がオフされており、Ａ系及びＢ系の２系で制御処理を行っている間に、今度はＡ系が故障したため、Ａ系の電源回路をオフにし、結局Ｂ系の電源回路もオフにすべき場合を示している。項目３は、Ｂ系が故障のため既に電源回路をオフされており、Ａ系及びＣ系の２系で制御処理を行っている間に、今度はＡ系が故障したため、Ａ系の電源回路をオフにし、結局Ｃ系の電源回路もオフにすべき場合を示している。

【０１０６】図１６は、故障した系の電源回路を強制的にオフする構成をＡ系を例に取って示した説明図である。この図において、２４ボルトの電源回路の０Ｖ端子と２４Ｖ端子との間にオンタイマリレー９０が接続されており、また、複数の接点により形成される接点群とＡ系電源リレー９１との直列接続体も両端子間に接続されている。

【０１０７】上記の複数の接点とは、オンタイマリレー９０のリレー接点９２、Ａ系電源リレー９１のリレー接点９３、Ｂ＝Ａのヘルシーリレー接点９４、Ａ＝Ｂのヘルシーリレー接点９５、Ｃ＝Ａのヘルシーリレー接点９６、Ａ＝Ｃのヘルシーリレー接点９７である。また、Ａ系電源リレー９１は交流１００ボルト電源の主接点９８を有している。

【０１０８】次に、図１６の動作を説明する。電源回路の投入時にはオンタイマリレー９０が数秒間励磁され接点９２をオンにするため、Ａ系電源リレー９１が強制的に励磁される。これにより接点９３がオンになり、また主接点９８がオンとなって、交流１００ボルトがコントローラに供給される。そして、Ａ系コントローラは接点９５，９７をオンにするが、これと同時にＢ系及びＣ系のコントローラも動作を開始して接点９４，９６をオンにする。したがって、Ａ系電源リレー９１の自己保持回路が形成され、オンタイマリレー９０が無励磁となった後もＡ系電源リレー９１の励磁状態が保持される。

【０１０９】この状態でＢ系及びＣ系がＡ系の故障を検出すると、接点９４，９６がオフとなるため、Ａ系電源リレー９１は無励磁となり主接点９８がオフとなって、故障系であるＡ系は健全系であるＢ系及びＣ系から完全に切断される。また、Ａ系及びＢ系の２系で制御処理中（Ｃ系が故障であるため、接点９６，９７は既にオフとなっている。）にＢ系がＡ系の故障を検出すると、接点９４がオフとなるため、Ａ系電源リレー９１は無励磁となり主接点９８がオフとなって、故障系であるＡ系の制御は停止される（これに伴って、健全系であるＢ系の制御も結局は停止される。）。同様に、Ａ系及びＣ系の２系で制御処理中（Ｂ系が故障であるため、接点９４，９５は既にオフとなっている。）にＣ系がＡ系の故障を検出すると、接点９６がオフとなるため、Ａ系電源リレー９１は無励磁となり主接点９８がオフとなって、故障系であるＡ系の制御は停止される（これに伴って、健全系であるＣ系の制御も結局は停止される。）。さらに、３系で制御処理中にＡ系が自己診断により自系の故障を検出した場合は、接点９５，９７がオフとなるため、この場合もＡ系電源リレー９１が無励磁となってＡ系の制御が停止される。

【０１１０】図１７は、各リレーの励磁状態及び各ヘルシーリレー接点のオンオフ状態の変化を示すタイムチャートであり、（ａ）は３系で正常動作中にＡ系が異常となった場合、（ｂ）はＡ系及びＢ系の２系で動作中にＡ系が異常となった場合を示している。

【０１１１】図１７（ａ）において、電源投入後に直ちにオンタイマリレー９０がオンになると共にＡ系電源リレー９１及びＣ系電源リレーがオンとなっている。そして、オンタイマリレー９０がオフとなった後、Ｂ系及びＣ系がＡ系の異常を検出したため接点９４，接点９６がオフとなってＡ系電源リレー９１をオフにする。さらに、この後Ａ系の接点９５，９７もオフとなる。

【０１１２】図１７（ｂ）において、先にＣ系の異常が検出され、Ｃ系電源リレーがオフとなった後（接点９６，９７も既にオフとなっている。）、Ｂ系がＡ系の異常を検出し、接点９４をオフにしてＡ系電源リレー９１をオフにしている。そして、この後Ａ系の接点９５もオフとなる。

【０１１３】次に、各系のコントローラが他系との間で照合動作を行う場合に、各系のタイマ同士の間におけるカウントタイミングのずれに起因する照合エラーを排除するための技術について説明する。

【０１１４】各系の基本クロック信号は互いに独立に生成されているので、各系のコントローラのタイマ同士の間では、１カウント分の時間差が発生し、タイマ処理状態が一致しない期間が存在する。例えば、メインプログラムにおいて、所定の基準時点から３秒経過後に或る動作を実行するように設定されている場合を考えてみる。この場合、Ａ系及びＢ系はそれぞれのタイマが「３」を表示した時点で、既述した入力又は出力の照合を行い、照合結果が一致した場合に上記の動作を実行することになる。

【０１１５】ところが、Ａ系及びＢ系の各タイマはそれぞれ独立して時間をカウントしているため、Ａ系タイマが「３」秒を表示した時点では、Ｂ系タイマがまだ「２」秒を表示しているという場合があり得る。両タイマはそのカウント値が３．０～３．９秒の期間に「３」秒を表示するようになっているが、例えば、Ａ系タイマが３．７秒をカウントした時点でようやくＢ系タイマが３．０秒をカウントした状態であったとすると、Ａ系タイマが３．０～３．６秒をカウントしている期間中は、Ａ系タイマは「３」秒を表示し、一方、Ｂ系タイマは「２」秒を表示していることになる。したがって、Ａ系タイマが「３」秒を表示した時点で上記の動作を実行すべく両系の照合を行うと、その照合結果は不一致となるため故障と判別されてしまうことになる。

【０１１６】図１８は、このような両系のタイマのずれに起因する誤検知を防止する技術についての説明するためのタイムチャートである。この図において、（ａ），（ｂ）はそれぞれＡ系タイマ及びＢ系タイマの処理状態を示す信号であり、ＣＡ1，ＣＡ2…、ＣＢ1，ＣＢ2…は１回目、２回目、…のカウントを示している。（ｃ），（ｅ）はスキャン番号が付されたスキャン信号Ｓ1～Ｓ9を示している。（ｄ），（ｆ）はＡ系タイマ及びＢ系タイマの実際の照合時における処理状態を示す信号ＴＡ1，ＴＢ１である。（ｇ）は上記の（ｄ），（ｆ）の信号の一致状態及び不一致状態を示す信号である。また、ｔ1はタイマの１カウントの間隔を示す時間であり、ｔ2はＡ系タイマとＢ系タイマの動作開始時点の差を示す時間であり、ｔ3は制御処理周期（スキャン周期）すなわちメインプログラムの走行周期を示している。

【０１１７】図１８（ａ），（ｃ）から明らかなように、Ａ系タイマの信号ＣＡ2が「１」になっている状態が検出されるのはスキャン信号Ｓ3の立ち上がり時点からであり、それ故、実際の照合時におけるＡ系タイマの処理状態は図１８（ｄ）の信号ＴＡ1によって示される。同様に、図１８（ｂ），（ｅ）から明らかなように、Ｂ系タイマの信号ＣＢ3が「１」になっている状態

が検出されるのはスキャン信号Ｓ5の立ち上がり時点からであり、それ故、実際の照合時におけるＢ系タイマの処理状態は図１８（ｆ）の信号ＴＢ1によって示される。そして、図１８（ｇ）に示されるように、信号ＴＡ1，ＴA2はスキャン信号Ｓ3，Ｓ4の期間においては互いに不一致の状態となっている。

【０１１８】したがって、もし上記のスキャン信号Ｓ3，Ｓ4の期間においてＡ系とＢ系との照合を行った場合には、両系のタイマ処理状態が一致しないために照合エラーとなって、故障を検知したと判断されてしまうことになる。しかし、この場合は実際にＡ系又はＢ系に故障が発生したわけではなく、上記の故障検知は誤検知である。

【０１１９】そこで、本実施形態ではこのような誤検知を防止するために、両系のタイマの処理状態の不一致を検出したとしても、所定時間の間はこの不一致を無効とする制御処理を行うようにしている。図１８の例では、タイマの１カウントの時間ｔ1がスキャン周期ｔ3よりも大きいので、少なくとも１カウント時間だけ待たないと、両系のタイマの処理状態は確実には一致状態とならない。例えば、ｔ1を１００ｍｓ、ｔ3を４０ｍｓとした場合に、３スキャンの間（Ｓ3，Ｓ4，Ｓ5）は不一致を検出したとしてもこの不一致を無効とする処理を行い、４スキャン連続で（Ｓ3～Ｓ6）不一致を検出した場合にはじめてこの不一致を有効とする処理を行うようにしている。図1･8の例では、タイマの１カウントの時間ｔ1がスキャン周期ｔ3よりも大きい場合につき説明したが、ｔ1がｔ3よりも充分に小さい場合は、１スキャン時間だけ待てば両系のタイマの処理状態は一致した状態となる。

【０１２０】

【発明の効果】以上のように、本発明によれば、各制御系が、現場機器との間の信号の入出力結果について、自系統側と１つの他系統側との間で一致するか否かについて共有メモリを用いて照合する機能を有し、全ての制御系の照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行するようにしており、また、自系統側又は照合相手の他系統側が正常状態又は故障状態のいずれにあるかをヘルシー回路を用いて検知する機能を有し、いずれかの系統のヘルシー回路から故障信号を入力した場合は制御動作を停止するようにしているので、簡単な構成によって、フェイルセーフ性を向上させることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態の構成を示すブロック図。

【図２】図１における入力ユニット８Ａ，８Ｂ、及びこの入力ユニットと信号の授受を行うＡ系コントローラ１Ａ，Ｂ系コントローラ１Ｂの構成を示すブロック図。

【図３】図２の入力ユニットの代表的な故障モードを示した図表。

【図４】図１における出力ユニット９Ａ，９Ｂ、及びこの出力ユニットと信号の授受を行うＡ系コントローラ１Ａ，Ｂ系コントローラ１Ｂの構成を示すブロック図。

【図５】図４の動作を説明するためのタイムチャート。

【図６】図４の出力ユニットの代表的な故障モードを示す図表。

【図７】図１におけるヘルシー回路１０Ａ，１０Ｂの構成図。

【図８】図８の動作を説明するためのタイムチャート。

【図９】図７におけるマイクロプロセッサ・ユニット２Ａの構成を示すブロック図。

【図１０】本発明の第２の実施形態の構成を示すブロック図。

【図１１】図１１の実施形態に係る電子踏切制御装置（鉄道用保安制御装置）を用いて構成した電子踏切制御システム（鉄道用保安制御システム）の構成図。

【図１２】図１０におけるヘルシー回路７９Ａ，７９Ｂ，７９Ｃの構成図。

【図１３】図１０の動作を説明するためのフローチャート。

【図１４】図１０のエラー処理が行われる主な場合を説明するためのフローチャート。

【図１５】図１０における各系のコントローラ内の電源回路をオフにする場合の態様を示す図表。

【図１６】図１０における各系のコントローラ内の電源回路をオフにするための構成図。

【図１７】図１６の動作を説明するためのタイムチャート。

【図１８】図１０における各系のコントローラが他系との間で照合動作を行う場合に、各系のタイマ同士の間におけるカウントタイミングのずれに起因する照合エラーを排除するための技術を説明するためのフローチャート。

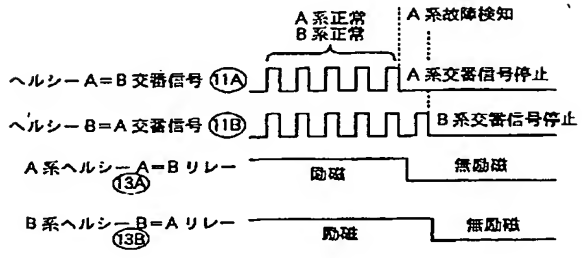
【図１９】従来の鉄道用保安制御装置の要部の構成を示すブロック図。

【符号の説明】

１Ａ，１Ｂ　Ａ系及びＢ系マイクロプロセッサ・コントローラ
２Ａ，２Ｂ　マイクロプロセッサ・ユニット
３Ａ，３Ｂ　記憶部
４Ａ，４Ｂ　記憶部
５Ａ，５Ｂ　入出力インタフェイス
６Ａ，６Ｂ　ＭＰＵバス
７Ａ，７Ｂ　Ｉ／Ｏバス
８Ａ，８Ｂ　入力ユニット
９Ａ，９Ｂ　出力ユニット
１０Ａ，Ｂ１０　ヘルシー回路
１１Ａ，１１Ｂ　出力回路
１２Ａ，１２Ｂ　トランス

１３Ａ，１３Ｂ　リレー
１４Ａ，１４Ｂ　ヘルシーリレー接点
１５Ａ，１５Ｂ　Ｉ／Ｏバスコントローラ
１６Ａ，１６Ｂ　共有メモリ
１７　リレー
１８　リレー接点
１９Ａ，１９Ｂ　抵抗
２０Ａ，２０Ｂ　フォトカプラ
２１Ａ，２１Ｂ　発光ダイオード
２２Ａ，２２Ｂ　フォトトランジスタ
２３Ａ，２３Ｂ　フォトカプラ
２４Ａ，２４Ｂ　発光ダイオード
２５Ａ，２５Ｂ　フォトトランジスタ
２６Ａ，２６Ｂ　故障診断回路
２７Ａ，２７Ｂ　信号入力回路
２８Ａ，２８Ｂ　比較照合回路
２９Ａ，２９Ｂ　チェック信号発生回路
３０Ａ，３０Ｂ　フォトカプラ
３１Ａ，３１Ｂ　発光ダイオード
３２Ａ，３２Ｂ　フォトトランジスタ
３３Ａ，３３Ｂ　フォトカプラ
３４Ａ，３４Ｂ　発光ダイオード
３５Ａ，３４Ｂ　フォトトランジスタ
３６Ａ，３６Ｂ　フォトカプラ
３７Ａ，３７Ｂ　発光ダイオード
３８Ａ，３８Ｂ　フォトトランジスタ
３９Ａ，３９Ｂ　抵抗
４０　ダイオード４０
４１　抵抗４１
４２Ａ，４２Ｂ　出力信号駆動回路
４３Ａ，４３Ｂ　故障検出回路
４４Ａ，４４Ｂ　チェック信号発生回路
４５Ａ，４５Ｂ　接点リードバック回路
４６Ａ，４６Ｂ　ダイオード
４７　制御処理手段
４８　交番信号発生手段
４９　カウンタ
５０　走行フラグ
５１　カウンタ
６１　第１の制御処理端末装置
６２　第２の制御処理端末装置
６３～６６　入出力処理端末装置
６７～７０　現場機器
７１Ａ，７１Ｂ，７１Ｃ　Ａ系、Ｂ系及びＣ系マイクロプロセッサ・コントローラ
７２Ａ，７２Ｂ，７２Ｃ　マイクロプロセッサ・ユニット
７３Ａ，７３Ｂ，７３Ｃ　メモリ部
７４Ａ，７４Ｂ，７４Ｃ　ＬＡＮ制御部
７５Ａ，７５Ｂ，７５Ｃ　Ｉ／Ｏバス・インタフェイス
７６Ａ，７６Ｂ，７６Ｃ　Ｉ／Ｏバス・インタフェイス
７７Ａ，７７Ｂ，７７Ｃ　入力ユニット
７８Ａ，７８Ｂ，７８Ｃ　出力ユニット
７９Ａ，７９Ｂ，７９Ｃ　ヘルシー回路
８０～８２　共有メモリ
８３　現場機器入力信号モジュール
８４　現場機器出力信号モジュール
８５Ａ1，８５Ａ2　出力回路
８６Ａ1，８６Ａ2　トランス
８７Ａ1，８７Ａ2　ダイオード
８８Ａ1，８８Ａ2　リレー
８９Ａ1，８９Ａ2　ヘルシーリレー接点
９０　オンタイマリレー
９１　Ａ系電源リレー
９２～９７　接点
９８　主接点
１０１Ａ，１０１Ｂ　マイクロプロセッサ・ユニット
１０２Ａ，１０２Ｂ　メモリ
１０３　クロック回路
１０４Ａ，１０４Ｂ　バス１０４
１０５　バス照合・交番信号出力回路
１０６　照合異常検出回路

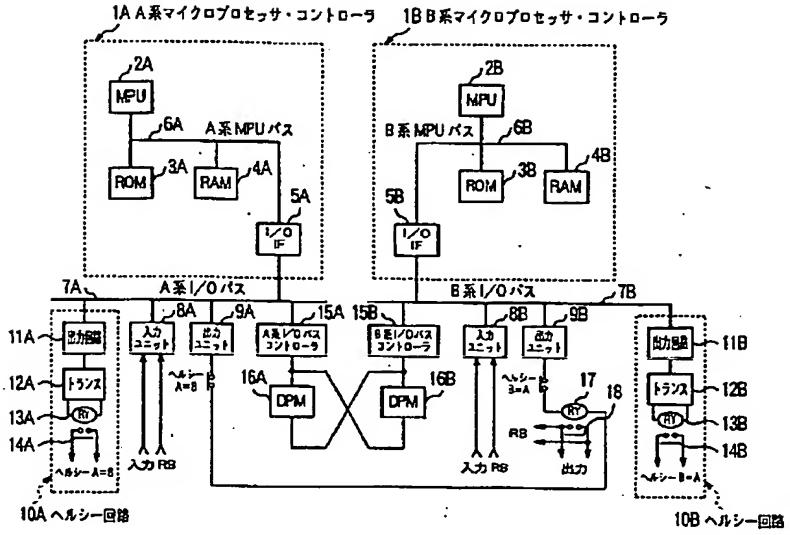
【図８】



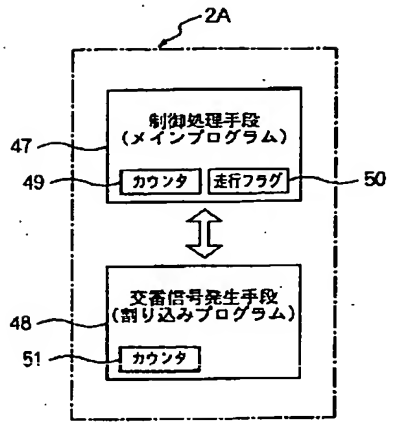
【図１５】

	A系		B系		C系		結果
	ヘルシーA=B	ヘルシーA=C	ヘルシーB=C	ヘルシーB=A	ヘルシーC=B	ヘルシーC=A	
1	0	0	1	0	1	0	多数決でA系のみを電源断
2	0	X_2	X_2	0	X_1	X_1	A系を電源断、B系も電源断
3	X_2	0	X_1	X_1	X_2	0	A系を電源断、C系も電源断

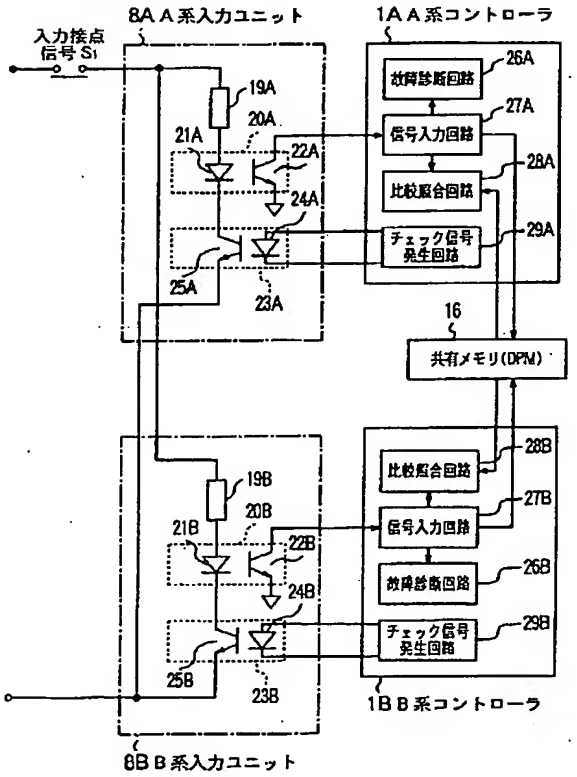
【図１】



【図９】



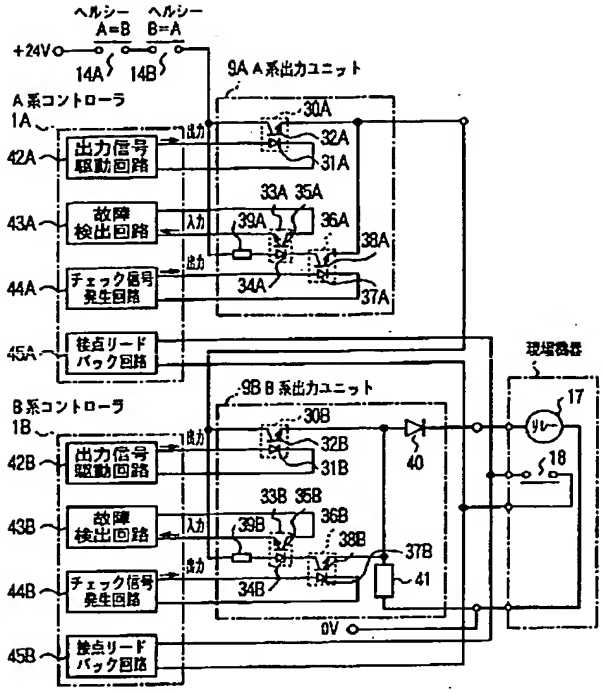
【図２】



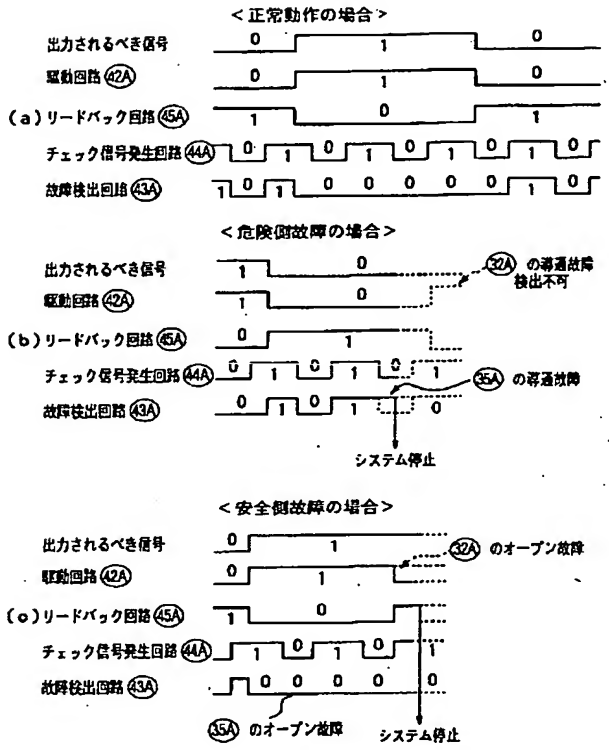
【図３】

項目	入力接点	チェック信号	信号入力回路㉗の状態	実際の状態	コントローラの判断
1	"0"＝開	0	0(正常)	正常	正常
2	"0"＝開	1	0(正常)	正常	正常
3	"0"＝開	0	0(故障)	潜在故障	正常
4	"0"＝開	1	0(故障)	潜在故障	正常
5	"0"＝閉	0	1(故障)	危険側故障	故障と判断
6	"0"＝閉	1	1(故障)	危険側故障	他系("0")との照合で故障を検知
7	"0"＝開	0(㉔のオン故障)	0(正常)	潜在故障	正常
8	"0"＝開	1(㉔のオン故障)	0(正常)	潜在故障	正常
9	"0"＝開	0(㉔のオフ故障)	0(正常)	潜在故障	正常
10	"0"＝開	1(㉔のオフ故障)	0(正常)	潜在故障	正常
11	"1"＝閉	0	0(故障)	故障	他系("1")との照合で故障を検知
12	"1"＝閉	1	0(故障)	故障	他系("1")との照合で故障を検知
13	"1"＝閉	0	0(正常)	正常	正常
14	"1"＝閉	1	1(正常)	正常	正常
15	"1"＝閉	0	1(故障)	故障	故障と判断
16	"1"＝閉	1	1(故障)	潜在故障	正常
17	"1"＝閉	0(㉔がオン故障)	1(正常)	故障	チェック中オフにならず故障と判断
18	"1"＝閉	1(㉔がオン故障)	1(正常)	潜在故障	正常
19	"1"＝閉	0(㉔がオフ故障)	0(正常)	故障	他系("1")との照合で故障を検知
20	"1"＝閉	1(㉔がオフ故障)	0(正常)	故障	他系("1")との照合で故障を検知

【図４】



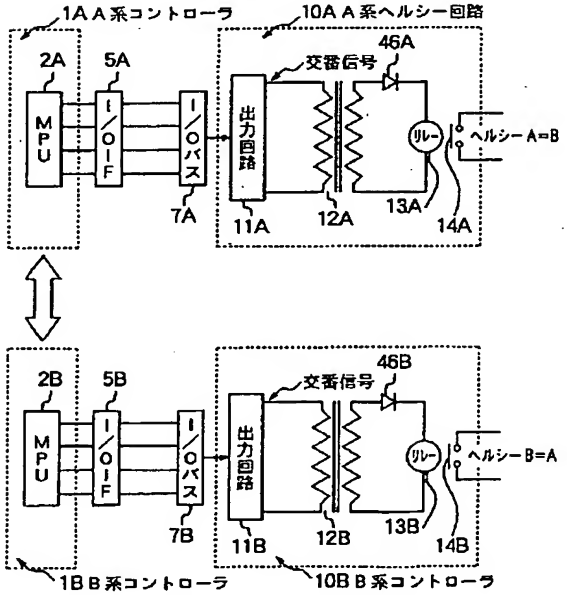
【図５】



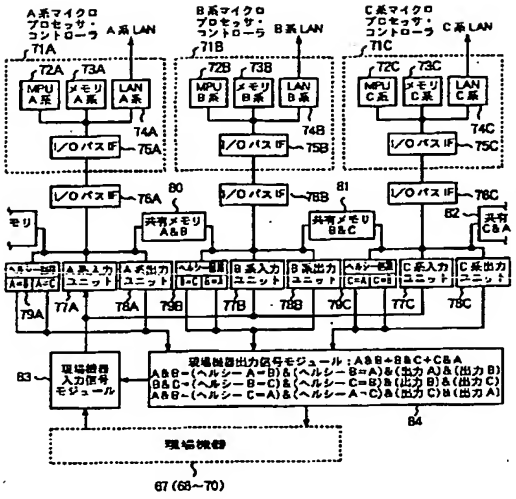
【図６】

項目	出力されるべき信号	リレー⑰の接点の状態	(42A) 駆動回路	(45A) R.B回路	(44A) チェック信号	(43A) 故障検出	コントローラの判断	実際の状態
1	0	無励磁	0：正常 ((32A) オフ)	1：正常 (⑰の反位置点をRB)	1：通常	1：正常	正常	正常
2					0：チェック中	0：正常		
3	0	無励磁	0：正常	0：故障	1：通常	1：正常	出力故障照合エラー	RB回路 (45A) が異常
4					0：チェック中	0：正常		
5	0	無励磁	0：正常	1：正常	1：通常	0：故障	故障検出回路 (43A) が故障	(43A) が"0"側に故障、又は (38A) がオープン
6					0：チェック中	0：正常		
7	0	無励磁	0：正常	1：正常	1：通常	1：正常	故障検出回路 (43A) が故障	(43A) が"1"側に故障、又は (32A) が導通
8					0：チェック中	1：故障		
9	0	無励磁	1：故障 ((32A) オン)	1：正常	1：通常	0：正常	駆動回路 (42A) が故障	(42A) が故障
10					0：チェック中	0：正常		
11	0	無励磁	1：故障 ((32A) オン)	1：正常	1：通常	1：故障	故障検出回路 (43A) が故障	(42A) の故障は検出不可、(43A)、(44A) の故障とみなす(2重故障)
12					0：チェック中	1：故障		
13	1	励磁	1：正常 ((32A) オン)	0：正常 (⑰の反位置点をRB)	1：通常	0：正常	正常	正常動作中
14					0：チェック中	0：正常		
15	1	無励磁	0：故障 ((32A) オープン)	1：正常	1：通常	1：正常	駆動回路 (42A) が故障	(42A) が故障
16					0：チェック中	0：正常		
17	1	励磁	1：正常 ((32A) オープン)	1：故障 ((45A) のオン故障)	1：通常	0：正常	RB回路 (45A) が故障照合エラー	接点溶着、又はRB回路 (45A) の故障
18					0：チェック中	0：正常		
19	1	励磁	1：正常	0：正常	1：通常	0：故障	正常	(43A) のこの故障は検出不可
20					0：チェック中	0：故障		
21	1	無励磁	0：故障 ((32A) オープン)	1：正常	1：通常	0：故障	他系との比較照合でエラー故障	(42A) の故障の後 (43A) の故障発生
22					0：チェック中	0：故障		

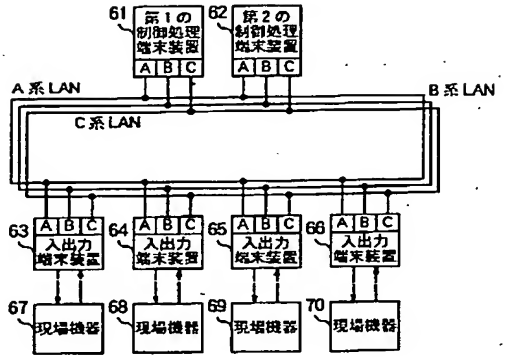
【図７】



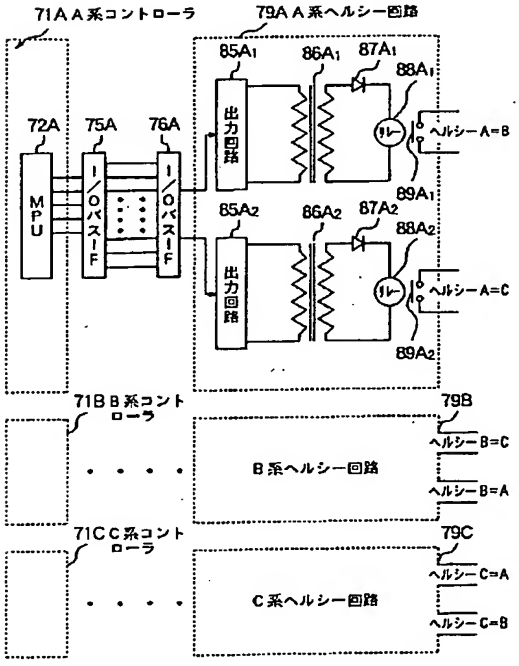
【図１０】



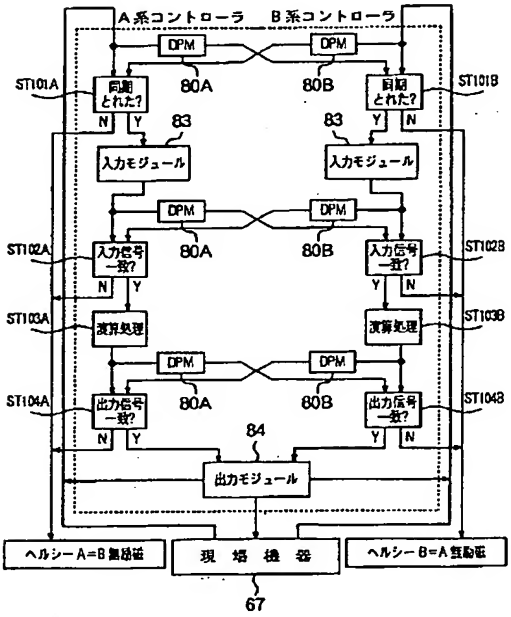
【図１１】



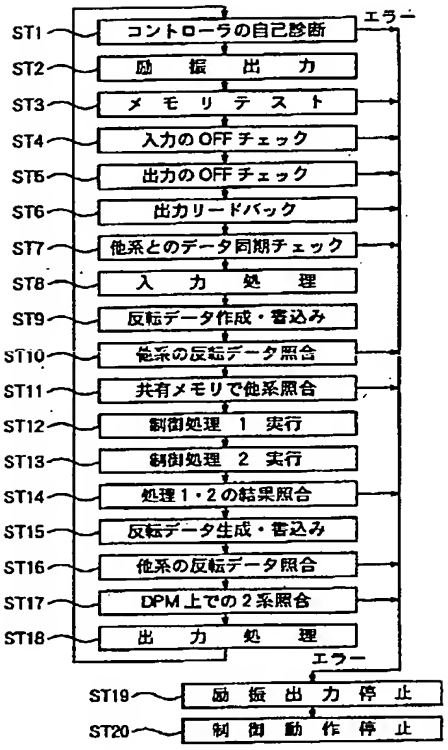
【図１２】



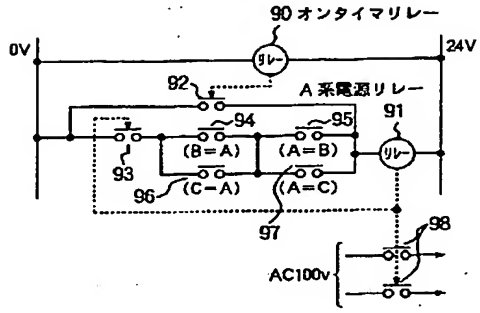
【図１３】



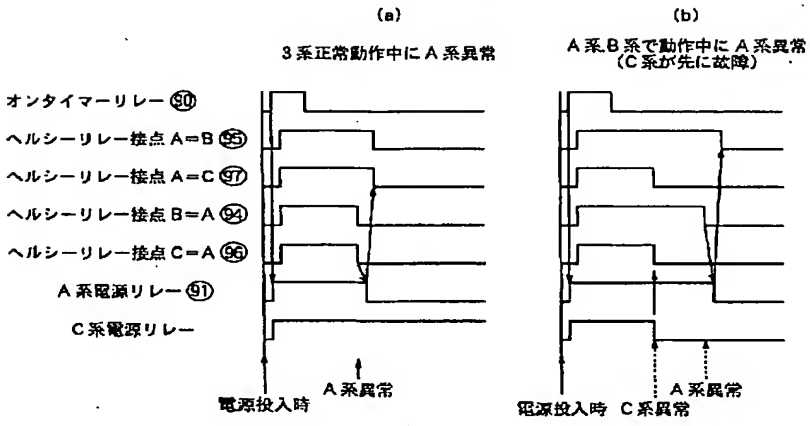
【図１４】


ST1
コントローラの自己診断
エラー
ST2
励　振　出　力
ST3
メ　モ　リ　テ　ス　ト
ST4
入力のOFFチェック
ST5
出力のOFFチェック
ST6
出力リードバック
ST7
他系とのデータ同期チェック
ST8
入　力　処　理
ST9
反転データ作成・書込み
ST10
他系の反転データ照合
ST11
共有メモリで他系照合
ST12
制御処理　1　実行
ST13
制御処理　2　実行
ST14
処理1・2の結果照合
ST15
反転データ生成・書込み
ST16
他系の反転データ照合
ST17
DPM上での2系照合
ST18
出　力　処　理
エラー
ST19
励　振　出　力　停　止
ST20
制　御　動　作　停　止

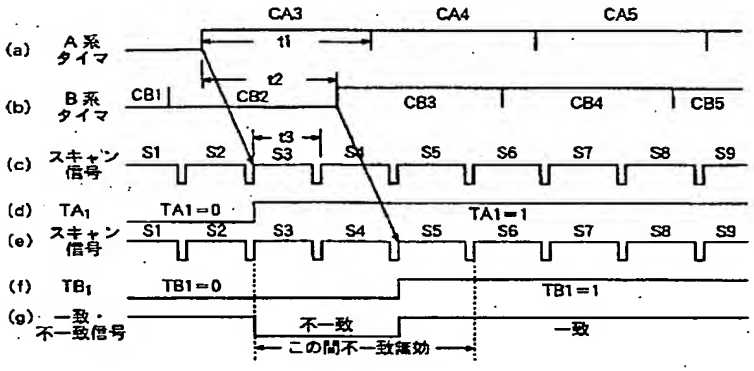
【図１６】


90 オンタイマリレー
0V
24V
リレー
92
A系電源リレー
91
94
95
(B=A)
(A=B)
93
96
(C=A)
(A=C)
97
98
AC100v

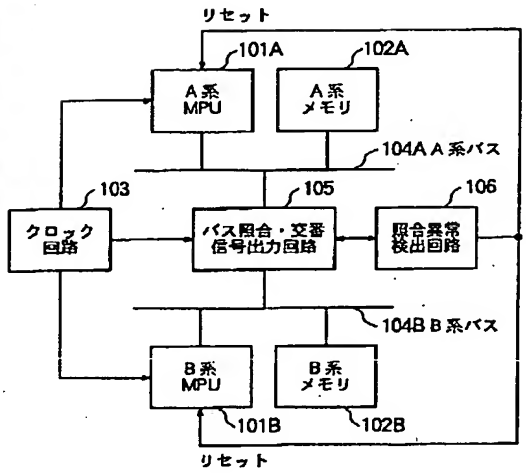
【図１７】


(a)
3系正常動作中にA系異常
(b)
A系B系で動作中にA系異常
(C系が先に故障)
オンタイマーリレー 90
ヘルシーリレー接点 A=B 95
ヘルシーリレー接点 A=C 97
ヘルシーリレー接点 B=A 94
ヘルシーリレー接点 C=A 96
A系電源リレー 91
C系電源リレー
電源投入時
A系異常
電源投入時
C系異常
A系異常

【図１８】



【図１９】



フロントページの続き

(72)発明者　目　黒　隆　之
東京都渋谷区代々木二丁目２番２号　東日本旅客鉄道株式会社内
(72)発明者　大　谷　祥　之
東京都渋谷区代々木二丁目２番２号　東日本旅客鉄道株式会社内
(72)発明者　磯　野　京　介
東京都渋谷区代々木二丁目２番２号　東日本旅客鉄道株式会社内
(72)発明者　永　島　暉　造
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(72)発明者　安　本　高　典
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

Ｆターム(参考)　5H209 AA09 BB07 CC05 DD04 EE06
GG04 SS01 SS04 SS07 TT00

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.